FIREHOUSE Software®
A Xerox Solution

FIREHOUSE Software
Web Edition Administrator's Guide

© 1993 - 2014
Xerox Government Systems, LLC. All rights reserved.
2900 100th St., Suite 309
Urbandale, IA 50322

WSpell ActiveX Spelling Checker © 1997 - 2002
Wintertree Software, Inc.
PDF Rasterizer.NET © 2001 - 2005
TallComponents BV

FIREHOUSE Software® is a registered trademark of Xerox Government Systems, LLC. All rights reserved. Microsoft, MS, MS-DOS, Microsoft Visual FoxPro, and Microsoft Access are registered trademarks. Windows is a trademark of Microsoft Corporation. CAMEO is a registered trademark. iPad is a registered trademark of Apple, Inc. All other products or services mentioned in this manual are identified by the trademarks or service marks of their respective companies or organizations. Xerox disclaims any responsibilities for specifying which marks are owned by which companies or organizations.

FIREHOUSE Software is protected by the copyright laws that pertain to computer software. It is illegal to make copies of the Software except for backups. It is illegal to rent, lease, sublicense, or otherwise transfer any of the materials. It is illegal to remove or obscure proprietary notices. It is illegal to duplicate and distribute the Software by any other means, including electronic transmission. To protect trade secrets contained in the Software, you may not decompile, reverse engineer, dissemble, or otherwise reduce the Software to human perceivable form. You may not modify, adapt, translate, rent, lease, or create derivative works based upon the Software or any part thereof.

Xerox warrants the original media are free from defects in material and workmanship, assuming normal use, for ninety (90) days from the date of purchase. Except for express warranty of the original media set forth above, Xerox grants no other warranties, express or implied, by statute or otherwise, regarding the media related materials, their fitness for any purpose, their quality, their merchantability, or otherwise. The liability of Xerox, under the warranty set forth above, shall be limited to the amount paid by the customer for the product. In no event shall Xerox be liable for any special, consequential, or other damages for breach of warranty.

© 2014 Xerox Government Systems, LLC.- Printed in the United States. All rights reserved. No part of this work covered by copyright hereon may be reproduced in any form by any means -- graphic, electronic, or mechanical -- including photocopying, recording, taping, or storage in any information retrieval system, without the written permission of the copyright owner.

FIREHOUSE Software License Agreement

Carefully read the following terms and conditions before installing software from **FIREHOUSE** Software. Only an Authorized Representative of the purchaser should install the software. Installing the software indicates acceptance of these terms and conditions specified in the License Agreement.

Xerox Government Systems, LLC and the party who installs this software ("you") hereby agree as follows:

1. **Licensed Software:** "Licensed Software" means the software component and modules ordered and paid for by you, as listed in Xerox's client database of licensed products, and as evidenced by your customer receipt. Licensed Software includes all documentation relating to our software. It also includes any upgrades, modifications, and customizations (collectively, "Improvements") to our software, should such Improvements be delivered to you at a later time.
2. **End Users:** "End User(s)" means (i) your employees with a need to access the Licensed Software; and (ii) third party consultants engaged by you who have a need to access the Licensed Software, and who are fulfilling legitimate business functions for you on your behalf.
3. **Materials:** This document contains links to downloaded files and applicable manual(s) relating to the Licensed Software.
4. **License Grant:** Xerox hereby grants a revocable, non-exclusive, non-transferable license to use the Licensed Software on a single microcomputer, in the United States of America. The number of End Users authorized to access the Licensed Software concurrently is reflected on your invoice and in this License Agreement. You may increase the maximum number of concurrent End Users by procuring additional licenses from Xerox based upon the then-current license fee schedule. You may not make use of any object code for any component(s) or modules(s) for which you have not expressly obtained a license for use under this Agreement. Any rights not expressly granted in this Agreement are expressly reserved. You agree not to (a) rent, lease, sublicense, assign or otherwise transfer the Licensed Software, including any of the materials or your rights hereunder, (b) remove or obscure our proprietary notices, (c) translate, alter, decompile or disassemble any of the materials, (d) copy any of the materials without our prior written consent, (e) use the software for other agencies. You shall have no right to access, copy or otherwise use the source code for software licensed under this license. You are prohibited from causing or permitting the reverse engineering, disassembly or decompilation of the software licensed under this license. You are prohibited from modifying, improving or otherwise enhancing the software licensed under this license.
5. **Terms:** This license is effective until terminated. You may terminate it at any time by destroying the materials and all copies of any material made from the original materials and notify Xerox immediately. This license terminates automatically upon breach of any of the conditions of this license. Upon termination, you agree to destroy all copies of the materials. Use of the materials without a valid license of the materials is unauthorized and may subject you to monetary penalties.
6. **Confidentiality:** You receive the right to use the Licensed Software and materials as specified herein, but you do not become the owner of the Licensed Software and materials. The Licensed Software and materials are exclusive property of Xerox and are protected by trade secret, copyright, and trademark law. You acknowledge that the materials are Xerox property and contain valuable, confidential, unpublished information developed by Xerox at a great expense. You agree to protect the materials from unauthorized reproduction, distribution, disclosure, or use of publication. You may not transfer any materials or software to anyone or entity without the written consent of Xerox authorized personnel.
7. **U.S. Government Restricted Rights:** The Licensed Software and documentation related thereto were developed at private expense and are provided with "RESTRICTED RIGHTS". Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR 52.227-14 and DFAR 252.227-7013 et seq. or its successor.

8. **Export Laws:** You may not export the Licensed Software and agree to comply with all laws, regulations, orders or other restrictions of the U.S. Export Administration Regulations.
9. **Warranty:** We warrant the downloadable files to be free from material defect in normal use for 90 days from the date of receipt of materials. We do not warrant the error-free operation of the Licensed Software contained in the downloadable files, or that such Licensed Software will meet your requirements. The Licensed Software is licensed "as is". We will, however, attempt to correct or bypass any actual reproducible and significant error in the software, provided you notify us and describe it in writing within 90 days from the date of receipt of the materials, and we will, within a reasonable time, at our option, provide either a corrected copy or work around instructions. This does not cover altered software or require us to customize our software to meet your hardware or operating system requirements. Section 11 specifies your exclusive remedy for any breach by us of this section. No dealer, company, or person is authorized to expand, alter this section or any other provision of this agreement. Any such agreement will not bind Xerox. XEROX MAKES NO OTHER WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, WITH REGARD TO THE SOFTWARE LICENSED UNDER THIS LICENSE, IN WHOLE OR IN PART. XEROX EXPLICITLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR A PARTICULAR PURPOSE. XEROX EXPRESSLY DOES NOT WARRANT THAT THE LICENSED SOFTWARE, IN WHOLE OR IN PART, WILL BE ERROR FREE, WILL OPERATE WITHOUT INTERRUPTION OR WILL BE COMPATIBLE WITH ANY HARDWARE OR SOFTWARE OTHER THAN THE EQUIPMENT. LICENSEE WAIVES ANY CLAIM THAT THE LIMITED WARRANTY SET FORTH IN THIS SECTION OR THE REMEDY FOR BREACH OF SUCH LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE.
10. **Limitation of Liability:** XEROX'S LIABILITY IN CONNECTION WITH THE LICENSED SOFTWARE UNDER THIS LICENSE, OR ANY OTHER MATTER RELATING TO THIS LICENSE WILL NOT EXCEED THE FEE THAT YOU ACTUALLY PAID TO XEROX FOR THE SOFTWARE GIVING RISE TO THE LIABILITY. REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL XEROX BE LIABLE TO YOU FOR ANY SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, INDEMNIFICATION, OR OTHERWISE, AND WHETHER OR NOT XEROX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. YOU ACKNOWLEDGE THAT XEROX HAS SET ITS FEES AND ENTERED INTO THIS LICENSE IN RELIANCE UPON THE LIMITATIONS OF LIABILITY AND THE DISCLAIMERS OF WARRANTIES AND DAMAGES SET FORTH IN THIS LICENSE, AND THAT THE SAME FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES.
11. **Remedy:** In the event that Xerox breaches this agreement, your sole remedy is to notify us of such breach within the applicable warranty period and we will at our sole option, either cure the breach or refund the license fee paid to us for the materials. In no event will Xerox be responsible for any damage beyond the amount of the license fee or for any indirect, special, incidental, consequential or similar damages or profits to you or any other person, or entity, regardless of the legal basis, even if Xerox has been advised of the possibility of such damages, except to the extent applicable state law specifically prohibits such exclusion.
12. **General (System Only):** This license shall be governed by laws of the State of Iowa. All prior correspondence oral or written including without limitation, all understandings with respect to the Licensed Software or materials relative thereto are hereby superseded. This license constitutes your and our entire agreement and understanding regarding the Licensed Software and materials relative thereto.
    General (Evaluation Only): This evaluation program is provided free of charge to the registered requestor of the evaluation software and is to be used solely as an evaluation copy.
13. **Software Maintenance Agreement:** 90 days free phone support is provided with purchase of FIREHOUSE Software. A separate software maintenance contract is available for an additional charge. This software maintenance contract is not mandatory but highly recommended. The annual maintenance contract includes phone support and program updates. The cost of the software maintenance contract is based on the type and number of modules installed. In the event that the 90 day free support period has expired and no software maintenance contract has been established, a "per call" fee will be billed to you for telephone or other technical support.

Technical support

FH® Technical Support:
Phone: 800-921-5300, option 2
support@firehousesoftware.com

Sales contacts

Jim Brandariz
Phone: 800-796-1614, 530-621-0981
Fax: 530-626-8582
Jim.Brandariz@firehousesoftware.com
AZ, CA, NV, OR, WA

Peter Eleftherakis
Phone: 888-362-4446, 508-362-4446
Fax: 508-362-5932
Peter.Eleftherakis@firehousesoftware.com
CT, MA, ME, NH, NY, RI, VT, Ontario

Mike Rogers
Phone: 888-941-3473, 214-504-0242
Fax: 214-504-0244
Mike.Rogers@firehousesoftware.com
AR, KS, LA, MO, MS, OK, TX

Forest Nace
Phone: 800-285-8685
Fax: 724-283-9086
Forrest.Nace@firehousesoftware.com
DE, IN, KY, MD, NJ, OH, PA, VA, WV

Roger DeDoncker
Rebecca Sanger
Phone: 800-921-5300, ext. 1
Fax: 515-288-4825
fhsales@xerox.com
AK, AL, CO, GA, FL, HI, ID, IA, IL, MI, MN, MT, NC, ND, NE, NM, SC, SD, TN, UT, WI, WY, International

Table of Contents

Introduction **1**

FH Web Edition features 1

New features 3

System requirements **4**

FH Web Edition servers 4

FH Web Edition client 5

Installing FH Web Edition server **6**

Manually copying the license file 6

Start the FH Web Edition License Manager 6

Verify that FH Web Edition Application Publishing Service and License Manager are running 6

Configuring the FH Web Edition server for Web clients **7**

Modifying the FH Web Edition Web pages 8

Example: Remove platform and configuration options from existing pages 8

Example: Create a page that loads a specific application 9

Example: Create a Web page with links to specific applications 10

Installing the Web files on a system other than the FH Web Edition server 10

Configuring redundant license servers 11

Three-server redundancy 11

License-file list redundancy 12

Set or change the LM_LICENSE_FILE variable 13

Configuring FH Web Edition to use a central license server 14

Opening the license manager port in a firewall 14

Configuring support for client keyboards and/or IMEs 15

Linux client keyboards supported 15

Macintosh OS X client keyboards supported 16

Windows CE client keyboards supported 16

Install keyboard layouts on a server running Windows Server 2008 17

Client keyboard mapping files 18

Keyboard/IME identifiers used by FH Web Edition 20

Configuring client keyboard options 20

Specifying layout text substitutions 21

Setting fallback layout text 21

Configuring multiple input locales 21
Administering user accounts **22**
Setting up user profiles 23
Setting file permissions 23
Setting up a network printer 24
Web Edition Connection Manager **25**
Access the FH Web Edition Connection Manager 25
Managing applications 25
Installing the application 25
Adding applications 26
Editing application properties 27
Duplicating an application 28
Renaming an application 28
Removing applications 28
Assigning launch parameters to users or groups 29
Managing sessions and processes 30
Terminating a session 30
Ending a process 30
Shadowing a session 30
Security options 32
Selecting SSL transport 32
Obtaining a trusted server certificate 32
Generate a CSR 32
Select the server certificate 33
Using an Intermediary SSL Certificate with FH Web Edition 34
Creating your own certificate authority 35
Import the trusted server certificate on a dependent host 35
Verify certificate filenames and location 36
Creating a CA Key and Certificate 36
Creating and signing server keys 38
Notifying users of a secure connection 39
Encrypting sessions 40
Modifying the host port setting 41
Standard authentication 42

Integrated Windows authentication 42
Enable integrated Windows authentication 43
Password caching on the host 43
Enable password caching on the host 44
Password caching on the client 44
Password change 45
Changing passwords at the next logon 45
Changing a password before expiration 46
Changing a password after expiration 46
Password change and Integrated Windows authentication 47
Shared account 48
Session reconnect 49
Setting the session termination 49
Disconnecting a session 50
Client time zone 50
Monitoring host activity 51
Viewing session information 51
Viewing process information 51
Displaying the status bar 52
Setting the broadcast interval 52
Session startup options 53
Applying group policy 53
Displaying progress messages 53
Logon scripts 54
Running logon scripts 54
Setting resource limits 55
Specifying the maximum number of sessions 55
Specifying the minimum physical and virtual memory 55
Session shutdown options 56
Specifying the session limit 56
Specifying the idle limit 56
Specifying the warning period 57
Specifying the grace period 57
Managing FH Web Edition servers from client machines 58

Keyboard shortcuts for the FH Web Edition Connection Manager 59
Applications tab 59
Sessions tab 59
Processes tab 59
General 59
Running FH Web Edition 60
Running FH Web Edition from a web browser 60
Running FH Web Edition from a computer's desktop 60
Install the FH Web Edition client 60
Launch FH Web Edition from the computer's start menu 61
(Windows) Create a shortcut to a FH Web Edition server 61
Launch FH Web Edition from a console window 61
FH Web Edition startup parameters 62
Create a FH Web Edition shortcut on Windows 64
Use shortcut parameters on Macintosh OS X 64
Create a FH Web Edition hyperlink 65
Resizing the client window 65
Uninstalling FH Web Edition 66
Uninstalling the FH Web Edition client from Windows 66
Uninstalling the FH Web Edition client from Linux 66
Uninstalling the FH Web Edition client on Macintosh OS X 66
Uninstalling the FH Web Edition client from Firefox 66
Uninstalling the FH Web Edition client from Internet Explorer 67
Uninstalling the FH Web Edition client from Apple Safari 67
Automatic client updates 68
Enabling automatic client updates 68
Updating the Mozilla Firefox plug-in 69
Disabling the FH Web Edition Update Client service 69
Updating the ActiveX control and the plug-in 69
Windows CE client 70
Determining if SEH and RTTI components exist on the device 70
Installing the Windows CE client 70
Running the Windows CE client from the Start menu 71
Running the Windows CE client from a shortcut 71

Running the Windows CE client from the FH Web Edition executable 71
Running FH Web Edition using command-line arguments 72
Editing the name or command-line options of a connection 73
Deleting a connection 73
Running a FH Web Edition connection 73
Uninstalling the Windows CE Client 73
Advanced topics 74
Load balancing 74
Independent hosts 75
Relay servers 75
Configure a FH Web Edition server to operate as a relay server 76
Relay server failure recovery 76
Dependent hosts 77
Configure a FH Web Edition server to operate as a dependent host 77
Administering relay servers and dependent hosts on different networks 78
Host selection 79
FH Web Edition server performance counters 80
Add FH Web Edition server performance counters to the Performance Monitor 81
Configuration requirements for delegation support 82
Client printing 84
Designating access to printer drivers 85
Designating access to printer drivers 85
Printer configuration 86
Printers Applet 86
Adding and removing printers 87
Adding a client printer 87
Removing a printer 87
Setting the default printer 87
Editing printer settings 88
Printing a test page 88
Changing a printer's driver 88
Resetting printer settings 89
Mapping printer drivers 89
Changing to a different printer driver 89

Forcing a printer to use the universal printer driver 90
Designating an additional driver 90
Removing printer driver mapping 91
Client printer naming customization 92
Customizing the client printer name 92
Enabling client clipboard 93
Enabling client sound, and client serial and parallel ports 93
Enabling client file access 94
Remapping client drives 95
Listing client drives sequentially starting at a given drive letter 95
Incrementing client drive letters by a fixed value 95
Hiding client drives 96
Hiding host drives 96
Mapped drives 96
Multiple monitor support 97
Obtaining the name of the client computer 97
Specifying the maximum color depth for FH Web Edition sessions 98
Disabling image compression 99
Application script support 99
Advanced session process configuration 100
Adding custom redirector settings for a specific application 102
Changing the default redirection settings 102
Example configuration 103
Proxy tunneling 105
Allowing HTTP CONNECT method tunnels using port 443 106
Support for Internet Protocol version 6 106
Enabling support for PAE 107
Performance auto-tuning 107
Log files 108
Selecting a new location for the log files 109
Setting the output level 109
Maintaining log files 110
Deleting log files 110
Backing up log files 110

Introduction

FH® Web Edition is the simple and secure application virtualization solution that extends the reach of **FIREHOUSE** Software to corporate network or the Web—without modifying a single line of code. FH Web Edition makes it easy to create a private cloud that allows authorized employees, business partners, and customers to securely access applications from anywhere, regardless of connection, location, client platform, or operating system.

FH Web Edition features

FH Web Edition contains a number of powerful features.

- **Network, remote dial-up, and remote Web accessibility.** FH Web Edition provides access to **FIREHOUSE** Software through the network, remote dial-up, or through Web access. This is managed through the FH Web Edition Connection Manager, and is transparent to the end user.
- **Cross-platform compatibility.** FH Web Edition provides access to any Windows application from virtually any client platform. FH Web allows **FIREHOUSE** Software to be run from desktop computers such as Mac, Windows, and Linux—allowing users to work in their preferred computing environments. Windows-based applications deployed through FH Web Edition look, feel, and function as if they were running on a Windows operating system, regardless of the client platform.
- **Client file access.** FH Web Edition supports seamless integration of client drives, including hard disk and mapped network drives. This allows users to access files stored on the client computer and to save files locally.
- **Host monitoring.** FH Web Edition provides real-time monitoring of individual FH Web Edition servers, control of individual clients and processes, and logout and shutdown for individual users.
- **User roaming.** Internal and remote users can sign in to a FH Web Edition server from any client workstation.
- **Automatic Windows Update and Hotfix Compatibility.** This feature automatically detects the locations of the internal operating system variables and functions used by FH Web Edition. This ensures that virtually every time the system is booted, users are able to start sessions and run published applications, regardless of what Windows Updates and Hotfixes are installed on the system.
- **Session shadowing.** The session-shadowing feature allows multiple users to view and control a single session and its applications. This feature allows help desk personnel and system administrators to help troubleshoot and debug user problems. Session shadowing may also be used for live collaboration.
- **Load balancing.** Load balancing distributes user sessions across multiple FH Web Edition servers. When load balancing is enabled, users can reconnect to a disconnected session running on any one of the load-balanced hosts.
- **Session reconnect.** With session reconnect enabled, FH Web Edition maintains client sessions on the server without a client connection. If a user deliberately disconnects from the server, or if the client's connection is lost due to network problems, the user's session

and applications remain running on the server for the length of time specified by the administrator.

- **Performance Counters.** Performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a server. FH Web Edition server performance counters allow administrators to monitor server activity from any machine with network access to a FH Web Edition server.
- **Proxy Tunneling.** Proxy tunneling allows users to connect to FH Web Edition server on the Internet through proxy servers.
- **Group Policy Support**. Using Microsoft's Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options.
- **SSL Security.** FH Web Edition provides support for Secure Socket Layer (SSL) as a method for communication between FH Web Edition clients and servers.
- **Session Timeout.** Through the FH Web Edition Connection Manager, administrators can specify time limits for the number of minutes that sessions are allowed to run on a FH Web Edition server.
- **Inactivity Timeout.** Through the FH Web Edition Connection Manager, administrators can specify time limits for the number of minutes of client inactivity.
- **Client Printer Name Customization.** Administrators can specify the format of client printer names and include information (including the user's name, the name of the session, and the client computer's IP address) in the name of the client printer.
- **Time Zone Redirection.** This option allows FH Web Edition sessions to run in the time zone of the client computer, regardless of the time zone that is selected on the FH Web Edition server.
- **Backward Compatible Client and Host.** This allows a client to connect to a FH Web Edition server when the major and minor versions of the client and server match but the revision (service pack) or build numbers do not.

New features

The following new server features are available with FH Web Edition 4.

- **Support for 64-bit Windows.** FH Web Edition supports the **FIREHOUSE** Software application running on x64 versions of Windows Server 2008, Windows 7, and Windows 8.
- **Automatic Client Updates.** Administrators can configure FH Web Edition to automatically update Windows clients when users connect to a FH Web Edition server that is running a newer version.
- **Simplified Client Printing.** Client printing has an updated, streamlined architecture with improved client compatibility, better integration with Windows hosts, faster session startup time, and support on 64-bit hosts.
- **Improved Application Compatibility.** FH Web Edition 4 has a simpler interface to the operating system that provides enhanced compatibility with both x86 and x64 applications.
- **Faster Application Startup.** Per-process CPU and memory usage overhead are greatly reduced. As a result, applications start more quickly and consume less memory.
- **Dynamic Display Resize.** FH Web Edition automatically adjusts the size of the session's desktop when the user reconnects to the session from a different device or changes the resolution of the client device.
- **Client Sound.** FH Web Edition supports sound capability for any application that uses PlaySound, sndPlaySound, or waveOut.
- **Client Serial and Parallel Ports.** FH Web Edition allows applications running on the host to access client machines' serial and parallel ports.

System requirements

FH Web Edition server and client machines require the following hardware and software.

FH Web Edition servers

The FH Web Edition server requires one of the following Windows operating systems:

- Windows Server 2008 Standard or Enterprise with Service Pack 2 (x86 and x64)
- Windows Server 2008 R2 Standard or Enterprise (x64)

Note:

- Where applicable, these platforms are supported with or without the Security Rollup Package.
- Right-to-left languages are not supported.
- FH Web Edition includes support for WoW64 (Windows 32-bit On Windows 64-bit) which allows 32-bit applications to run on 64-bit versions of Windows.
- FH Web Edition administrators must have administrative rights on the server to perform the installation, and the server must have TCP/IP as a network protocol.
- FH Web Edition supports VMware ESXi and Hyper-V in Windows Server 2008 R2.
- Microsoft Internet Information Server (IIS) must be available to set up the server for browser deployment of FH Web Edition.
- The color depth of the client and server must be greater than 25—16 million or greater is recommended.
- The memory and CPU requirements of a FH Web Edition server are determined by the applications that are published and the number of users accessing the system. In general, a FH Web Edition server can support 12 “heavy” users/500 MHz CPU and 25 “light” users/500 MHz CPU. (“Heavy” is defined as a user running one or more large applications with continuous user interaction. “Light” is defined as a user running one application with intermittent user interaction.)
- FH Web Edition supports a maximum round-trip latency of 500 milliseconds.

FH Web Edition client

Users can connect to a FH Web Edition server from any computer that supports a FH Web Edition client. FH Web Edition allows the following platforms:

- Windows Server 2008

  Both the x86 and x64 versions of this operating systems is fully supported.

  > **Note:** Extended support for environments and products that have reached Microsoft's end of mainstream support is available if you subscribe to either **FIREHOUSE** Software's Gold or Platinum support program. Information on the FH Support Programs is available at http://www.firehousesoftware.com/pdf/FH_Support_Program.pdf.

- Red Hat Linux (Enterprise Linux 4 and 5) and SUSE Linux (Enterprise Desktop 10.)

  Only a 32-bit client is provided. When installing this client on a 64-bit operating system, additional 32-bit dependencies may need to be installed. Consult your distribution's documentation for details on how to do this. Installing the client through a meta-packager such as yum automatically fetches and installs these dependencies for you.

- Mac OS 10.4 and later.

- Windows CE 4.2 or later on Mitsubishi's TX120 device, and Mintwave's ACC-Lite and ACC-mini devices.

  SEH (the C++ Structured Exception Handling component) and RTTI (the Run-Time Type Information component) are required to run FH Web Edition on a Windows CE device. To determine if these components exist on the device, open `ceconfig.h` in the Windows folder.

  On a Windows CE 4 device, if the following lines are included in this file:

  ```
  #define COREDLL_CRT_RTTI 1
  #define COREDLL_CRT_CPP_SEH 1
  ```

  then RTTI and SEH are supported.

  On a Windows CE 5 device, if the following line is included in this file,:

  ```
  #define COREDLL_CRT_CPP_EH_AND_RTTI 1
  ```

  then RTTI and SEH are supported.

FH Web Edition supports the following browsers:

- Internet Explorer 10.0 or later

  > **Note:** FH Web Edition is supported on Internet Explorer 11.0 in compatibility mode.

- Mozilla Firefox 24 Extended Support Release (ESR) or later, on Windows and Linux
- Apple Safari 5.0.6 or later, on Mac OS X

> **Note:** Only the Windows clients and the Mozilla Firefox and Internet Explorer browsers are fully supported. **FIREHOUSE** Software technical support will provide best-effort support for the other clients. FH Web Edition is not supported on Google Chrome.

Installing FH Web Edition server

FH Web Edition is delivered as a self-extracting executable, and can be installed by double-clicking the executable. For the FH Web Edition Application Publisher service to start correctly, you need to request a temporary license from support@firehousesoftware.com.

Following the installation, you need to restart the host and verify that the FH Web Edition Application Publishing Service and the FH Web Edition License Manager are running.

Manually copying the license file

After receiving your temporary license, copy your license file into the Programs directory in the FH Web Edition install path. If you have configured FH Web Edition to use a central license server, copy the license file to the license server.

Information on configuring the license server is available in **Configuring FH Web Edition to use a central license server**, on page 14.

Once the license file is copied over, you need to stop and restart the FH Web Edition License Manager.

Start the FH Web Edition License Manager

1. Choose **Start** → **Control Panel** → **Administrative Tools**.
2. Double-click **Services**.
3. From the list of services, select **FH Web Edition License Manager**.
4. Click **Start**.

Verify that FH Web Edition Application Publishing Service and License Manager are running

1. Choose **Start** → **Control Panel** → **Administrative Tools**.
2. Double-click **Services**.
3. Find **FH Web Edition Application Publishing Service** and **FH Web Edition License Manager** in the list of services.
4. Verify that these services display **Started**, and that the startup is **Automatic**.

   Tip: To set startup preferences for the FH Web Edition server, choose **FH Web Edition Application Publishing Service** from the list, click **Startup**, and then select the options you want to apply to the FH Web Edition server.

Configuring the FH Web Edition server for Web clients

The FH Web Edition server setup installs the FH Web Edition Web files under `C:\Program Files\ACSXerox\FH Web Edition\Web`. If Microsoft Internet Information Services (IIS) is detected during installation, a virtual directory will be created in IIS that points to the FH Web Edition Web files. If IIS is not available, administrators need to manually host the FH Web Edition Web folder contents on the specified Web server.

For more information on virtual directories in IIS, see Using Virtual Directories (IIS 6.0), at http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/8c110149-8060-4dd7-9bdb-e262c21483dd.mspx?mfr=true

Administrators can edit the FH Web Edition HTML pages to modify default options and limit which clients are available to users. During installation, the initial Web page is set to `index.html`. Users accessing the host from a Web browser should be directed to the FH Web Edition logon page.

Example: `http://hostname/fhweb/index.html`

The `clients.html` page detects the user's platform and browser, but it lists all the FH Web Edition clients that can be installed on the user's computer. The `allclients.html` page lists all FH Web Edition clients no matter which client operating system is detected.

In addition to `logon.html`, `clients.html`, and `allclients.html`, the following HTML pages are located in the FH Web Edition Web folder:

HTML page	Description
`index.htm`	Default landing page.
`installCE.html`	Installation page for the Windows CE client.
`installLinux.html`	Installation page for the Linux client. (`FH_Web.linux.rpm`)
`installMac.html`	Installation page for the Mac OS X client. (`FH_Web.mac.dmg`)
`installWindows.html`	Installation page for the Windows client. (`FH_Web.windows.exe`)

Modifying the FH Web Edition Web pages

You can use the above HTML pages as-is to install and run FH Web Edition from its supported operating systems and browsers. You can also customize these pages or create new pages to meet your specific needs. Modifications can be simple cosmetic changes that modify the appearance, text, or images of the pages. Changes can also be as complex as pages that are dynamically generated by Web applications. The following examples illustrate a few of the ways you can customize FH Web Edition's Web pages.

Example: Remove platform and configuration options from existing pages

You can remove links to the client for Windows CE.

1. Open `allclients.html` or `clients.html` in a text editor.
2. Delete the following lines from the file:

```
else
{
   document.write('<a href="installCE.html">Windows CE Client</a><br>');
}
```

3. Save the file.

You can also prevent the embedded windows option from being presented to Internet Explorer users

1. Open `allclients.html` or `clients.html` in a text editor.
2. Locate the following lines:

```
if(browser.msie)
{
document.write('Microsoft ActiveX Control: <a href-
f="logon.html?direct=true">Loose</a> | <a href-
f="logon.html?direct=true&embed=true">Embedded</a><br>');
}
```

3. Change the lines to:

```
if(browser.msie)
{
document.write('Microsoft ActiveX Control: <a href-
f="logon.html?direct=true">Loose</a><br>');
}
```

4. Save the file.

Example: Create a page that loads a specific application

`Logon.html` lets users create their own hyperlinks and specify whatever FH Web Edition options they like. In some cases, you may not want users to have this capability.

Example: You may want to prevent users from opening any application or file on the host computer, and instead provide a page that loads a specific application with a fixed set of options.

When specifying the application, you can use the display name that appears in the FH Web Edition Connection Manager or the fully qualified path to the application.

You can allow users to only run a specific application with specific options.

1. Open `logon.html` in a text editor.
2. Replace all instances of `GetVarDecoded("variable")` with either an empty string `("")` or the desired value for the parameter.
3. For the `app` variable, enter the application's display name that appears in the FH Web Edition Connection Manager.

   Example:
   ```
   var app = "Wordpad";
   var args = "";
   ```

   Or, enter the fully qualified path to the application.

   Example:
   ```
   var app = "C:\\Program Files\\Windows NT\\Accessories\\wordpad.exe";
   var args = "";
   ```
4. Save the file.
5. (Optional) Rename the file.

   Example: `wordpad.html`

Caution: When using a fully qualified path, any application-specific arguments must be specified using the `var args` parameter, regardless of whether or not the application was published through the FH Web Edition Connect Manager.

Note:

- The plug-in will not run if Microsoft Internet Information Server (IIS) 6.0 is installed on a FH Web Edition server running Windows Server 2008, unless you modify IIS to serve a document with an extension that does not have a registered MIME type on that server. For more information, see Microsoft Knowledge Base article 326965, IIS 6.0 does not serve unknown MIME types, at http://support.microsoft.com/default.aspx?scid=kb;en-us;326965.
- For FH Web Edition purposes, type `.xpi` in **Extension** on Windows systems and `.dmg` on Mac systems. In **MIME Type** , type `application/octet-stream`. Restart the World Wide Web Publishing Service on the Web server after making

this change.

Example: Create a Web page with links to specific applications

You can create a page with links to Wordpad and Windows Explorer.

Note: FH Web Edition options are specified in hyperlinks to the `logon.html` page. When users click these links, `logon.html` reads these options from the hyperlink and loads the appropriate client with the specified options.

1. Open a new or existing Web page in an HTML editor.
2. In the editor, click **Insert Hyperlink**.
3. Enter the URL to a Wordpad document:

   Example:
   ```
   http://hostname/fhweb/logon.html?mode=embed&app=C:\Program%20Files\
   Windows%20NT\Accessories\wordpad.exe&args=C:\Users\Public\
   Public%20Documents\welcome.rtf
   ```

4. Enter display text for the hyperlink,

   Example: `Welcome`

5. Repeat steps 2-4 to create a link to Windows Explorer.

   Example:
   ```
   http://hostname/fhweb/logon.html?mode=embed&app=C:\Windows\System32\explorer.exe
   ```

6. Save the file and add it to your Web server path.

Installing the Web files on a system other than the FH Web Edition server

You can install the FH Web Edition Web files on a system other than the FH Web Edition server.

1. Copy the contents of the `\Program Files\ACSXerox\FH Web Edition\Web` directory to the appropriate Web server.
2. Edit the `logon.html` page on the Web server and add the following statements, inserting the address of the FH Web Edition server in place of `hostname`.

   ```
   if (host.length == 0)
   {
   host="hostname";
   }
   ```

Configuring redundant license servers

If you wish to use redundant servers, select stable systems as server machines. Do not pick systems that are frequently rebooted or shut down. Redundant license server machines can be any supported FH Web Edition servers. These servers must have excellent communications on a reliable network and need to be located in the same subnet. Avoid configuring redundant servers with slow communications or dial-up links.

FH Web Edition supports two methods of redundancy:

- Through a set of three redundant license servers.
- Through a license-file list in the `LM_LICENSE_FILE` environment variable.

Note: The FH Web Edition License Manager service should be disabled on secondary servers of three-server redundant license servers and central license servers.

Three-server redundancy

With three-server redundancy, if any two of the three license servers are up and running, a "quorum" of servers is established, and the system is functional and serves its total complement of licenses.

Three-server redundancy is designed to provide hardware failover protection only and does not provide load-balancing. This is because with three-server redundancy, only one of the three servers is "master" and capable of issuing licenses.

You must provide the hostnames of the three FH Web Edition servers, as well as the hostIDs (Ethernet addresses, in most cases) for each. The port of the license server (example: 27000) must also be appended to each server line, if it is not already listed.

Example: Below is an example of a three-server redundant license file that Xerox supplies after registering online.

```
SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
DAEMON blm
INCREMENT session blm 4.0 31-dec-2010 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 4.0 31-dec-2010 uncounted D1D222D031C4 \
HOSTID=ANY
```

The three-server license file needs to be copied to each of the three license servers.

Lastly, you must point the FH Web Edition server to the license server. This can be done in two different ways: either by copying the license to each FH Web Edition server and editing it to use `USE_SERVER`, or by adding each server to the environment variable.

Example: A license that is edited to use `USE_SERVER`.

```
SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
USE_SERVER
```

With the second option, add each server to the environment variable, using commas to separate the servers.

Example: `LM_LICENSE_FILE = 27000@wilson,27000@piper,27000@caspian`

Restart the FH Web Edition Application Publishing Service and the FH Web Edition License Manager on the "master" server first (`wilson`, in the example above), then on the secondary and tertiary servers.

We recommend running Flexera's `lmtools` application to check the status of the redundant license servers once all three servers are up and running. Launch `lmtools.exe` and select the **Server Status** tab. Click **Perform Status Enquiry** and verify that your servers are "up."

You can obtain `lmtools` from the Programs directory (`\FH Web Edition\Programs`) or from http://www.globes.com/support/fnp_utilities_download.htm#downloads. The `lmtools` application is included for diagnostic purposes. Any questions on its functionality should be directed to Flexera.

License-file list redundancy

As an alternative to three-server redundancy, license-file list redundancy is available when there is limited system administration available to monitor license servers, when load-balancing is required for applications located far apart (example: Chicago and Tokyo), or when two or more license servers are required.

With license-file redundancy, each one of a group of license servers serves a subset of the total licenses. This method does not provide true redundancy in the way three-server redundancy does.

Set the `LM_LICENSE_FILE` environment variable to a list of license files, where each license file points to one of the license servers. FH Web Edition attempts a license checkout from each server in the list, in order, until it succeeds or gets to the end of the list. The actual licenses are generated from the product codes. Unlike with three-server redundancy, the server machines can be physically distant. The license servers on both servers need to be running.

Example: If ten licenses are wanted, you need to request two sets of product codes with a count of five for each set from your **FIREHOUSE** Software sales representative.

The sample license files will look like:

License 1 for Chicago:

```
SERVER chicago 00508BFE7FFE 27000
DAEMON blm
INCREMENT session blm 4.0 permanent 5 DF9C8F5ADF34 HOSTID=ANY \
   user_info="Joe User joeu@mycompany.com" ISSUER="Affiliated Computer Services, Inc \
   Corporation" ISSUED=17-feb-2010 NOTICE="Copyright (C) \
   1996-2010 Affiliated Computer Services, Inc. All Rights Reserved" ck=142 \
   SN=12865-AA
INCREMENT any_app blm 4.0 permanent 5 1DF84A360E8F HOSTID=ANY \
   user_info=" Joe User joeu@mycompany.com " ISSUER="Affiliated Computer Services, Inc \
   Corporation" ISSUED=17-feb-2010 NOTICE="Copyright (C) \
   1996-2010 Affiliated Computer Services, Inc. All Rights Reserved" ck=84 \
   SN=12865-AA
```

License 2 for Tokyo:

```
SERVER tokyo 00508BF77F7E 27000
DAEMON blm
INCREMENT session blm 4.0 permanent 5 16BE40E1D98D HOSTID=ANY \
   user_info="Joe User joeu@mycompany.com" ISSUER="Affiliated Computer Services, Inc \
   Corporation" ISSUED=17-feb-2010 NOTICE="Copyright (C) \
   1996-2010 Affiliated Computer Services, Inc. All Rights Reserved" ck=142 \
   SN=12865-AA
INCREMENT any_app blm 4.0 permanent 5 6DB6F3E402DF HOSTID=ANY \
   user_info=" Joe User joeu@mycompany.com " ISSUER="Affiliated Computer Services, Inc \
   Corporation" ISSUED=17-feb-2010 NOTICE="Copyright (C) \
   1996-2010 Affiliated Computer Services, Inc. All Rights Reserved" ck=84 \
   SN=12865-AA
```

Set or change the LM_LICENSE_FILE variable

The administrator of the `Chicago` server should set `LM_LICENSE_FILE` to `27000@chicago;27000@tokyo`, where `27000` represents the port that the license servers in Chicago and Tokyo are running. This directs the license engine to first attempt license checkouts from `Chicago`. If unsuccessful, it will attempt to checkout from `Tokyo`.

The administrator of the `Tokyo` server should set `LM_LICENSE_FILE` to `27000@tokyo;27000@chicago`. This directs the license engine to first attempt license checkouts from `Tokyo`. If unsuccessful, it will attempt to checkout from `Chicago`.

Note: As with three-server redundancy, we recommend running `lmtools` to verify the status of the redundant license servers once all servers are up and running.

1. To view or change the current environment variables, right-click **My Computer**, and then select **Properties**.
2. Click the **Advanced** tab, and then click **Environment Variables**.
3. Under **System variables**, select `LM_LICENSE_FILE`, and then click **Edit**.
4. Change **Variable value** from `C:\Program Files\ACSXerox\FH Web Edition\Programs` to reflect the new redundant servers.

   Note: Separate the license server names with a semicolon (;). FH Web Edition attempts the first server in the list. If that fails for any reason, the second server is tried.

5. Restart the FH Web Edition Application Publishing Service.

Configuring FH Web Edition to use a central license server

You can use two methods for configuring FH Web Edition to use a license server that serves multiple machines. In the following examples, `machine550` is the name of the license server, and `machine-w2k` is the name of the FH Web Edition server. We recommend stopping the FH Web Edition License Manager on the FH Web Edition server before getting started. The License Manager should be disabled on all secondary servers of the central license server.

1. Choose **Start → Control Panel → Administrative Tools**.
2. Double-click **Services**.
3. From the list of services, select **FH Web Edition License Manager**.
4. Click **Stop**.

Once you have stopped the FH Web Edition License Manager on the FH Web Edition server, do one of the following methods for configuring a central license server:

- On the FH Web Edition server, place `port@host` (example: `27000@machine550`) in the `LM_LICENSE_FILE` environment variable instead of the path to the license file. FLEXnet Publisher's `LMTOOLS.EXE` reports that the license file on `machine550` is being read correctly.
- On the FH Web Edition server, place `USE_SERVER` directly after the `SERVER` line in the license file on the FH Web Edition server. This is essentially the same as the preceding method, but the change to the environment variable is not required.

Example: The permanent license file (example: `license.lic`) on FH Web Edition server (`MACHINE-W2K`) would appear as follows:

```
SERVER machine550 00d0b74f4023
USE_SERVER
```

Opening the license manager port in a firewall

If there is a firewall between the FH Web Edition servers and the license server, the ports for FLEXnet (`27000`, by default) and for the license manager (`BLM`) need to be open in the firewall. For the license manager, add

```
port=<port#>
```

to the license on the license server for a specific port. (Unless you manually assign a specific port number, an ephemeral port number is used.)

```
EXAMPLE:
SERVER caspian 000476BA8F74 27000
DAEMON BLM port=5678
INCREMENT session blm 4.0 31-dec-2010 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 4.0 31-dec-2010 uncounted D1D222D031C4
HOSTID=ANY
```

Configuring support for client keyboards and/or IMEs

Windows uses input languages, keyboard layouts, Input Method Editors (IME), and code pages to map keys on a keyboard to the characters on the display. When a key is pressed on the client's keyboard, FH Web Edition sends a key code to the host, which translates the key code into a Windows input message using the session's active keyboard layout. The FH Web Edition setup configures the host to support clients that use the same operating system, keyboard, and/or IME as the host. FH Web Edition supports clients with different operating systems and keyboards with keyboard mapping files.

The following section describes mechanisms and procedures to manage keyboards and IMEs in sessions on client computers that do not match the host system.

Linux client keyboards supported

Linux Keyboard Layout Name (s)	Linux Keyboard Layout	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S. English	us	English (United States)	US	00000409	us.kbm
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	jp.kbm
French	fr	French (France)	French	0000040C	fr.kbm
Belgian (be-latin1)	be	French (Belgian)	Belgian French	0000080C	be.kbm
German, German (Latin1), German (Latin1 with no dead keys)	de	German (Germany)	German	00000407	de.kbm
Polish	pl	Polish	Polish (214)	00010415	pl.kbm
Brazilian (ABNT2)	br	Portuguese (Brazil)	Portuguese (Brazilian ABNT2)	00010416	br.kbm

*See the client keyboard mapping files section for more information.

Macintosh OS X client keyboards supported

Mac OS X Keyboard Layout Name	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S. English	English (United States)	U.S. International	00000409	us.kbm
French	French (France)	U.S. International	0000040C	fr.kbm
German	German (Germany)	U.S. International	00000407	de.kbm

*See the client keyboard mapping files section for more information.

Note: Due to physical differences between the Macintosh OS X and Windows keyboards, the Macintosh OS X keyboard mapping files use the U.S. International Windows keyboard layout to translate a majority of the keys to Windows applications.

Windows CE client keyboards supported

Windows CE Keyboard Layout Name	Windows CE VM Language	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S. English	en	English (United States)	US	00000409	internal
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	ja_JP.kbm
French	fr	French (France)	French	0000040C	fr.kbm
German	de	German (Germany)	German	00000407	de.CH.kbm

*See the client keyboard mapping files section for more information.

Windows clients (including the native Windows Client, the ActiveX Control, and the Plug-in) support any keyboard that the FH Web Edition server has drivers for.

Install keyboard layouts on a server running Windows Server 2008

Before clients can use keyboards and/or IMEs that are different from the host's, the files used to support them must be installed on the FH Web Edition server. In most cases the layouts are copied during the installation of the operating system, but East Asian and right-to-left input languages are not.

1. Choose **Start** → **Control Panel**.
2. Double-click **Regional and Language Options**.
3. Click the **Keyboard and Languages** tab.
4. Click **Change keyboards**.
5. In the **Text Services and Input Languages** window, click **Add**.
6. In the **Add Input Language** window, select the languages you want.
7. Click **OK**.
8. In the **Text Services and Input Languages** window, click **Apply**.
9. Click **OK**.

Client keyboard mapping files

The FH Web Edition client uses keyboard mapping files on Linux, Macintosh OS X, and Windows CE to ensure that the proper keyboard layout is loaded on the host, and that the correct key codes are sent for each key press and release. Keyboard mapping files provide support for new keyboards to be added by simply copying a new keyboard mapping file to the client. Keyboard mapping files are installed into the `/etc/fhweb-client/kbd` directory of these clients. An internal version of the `us.kbm` keyboard mapping file is used if a keyboard mapping file is not found.

These clients can automatically load keyboard mapping files based on information obtained from the operating system.

Client OS	Native install	Browser plug-in install	Default layout	Layout obtained by
Linux	`/etc/ FH_Web/kbd`	`~/.mozilla/ FH_ Web/kbd`	U.S. English	Environment variable or automatically from the OS
Mac OS X	`/etc/ FH_Web/kbd`	`/etc/ FH_Web/kbd`	U.S.	Environment variable or automatically from the OS
Windows CE	`/ACSXerox/FH Web Edition Client/kbd`	N/A	en	Automatically from the OS

Environment Variable	Description
`FHWEB-CLIENT_KBD_FILE`	Specifies the fully qualified path name of the mapping file to use. If specified, this overrides all other means of obtaining the filename path. **Example:** On Linux, `FHWEB-CLIENT_KBD_FILE=/home/someuser/KeyMappingFiles/MyCustomKeyMappingFile.kmf` causes that exact file to be loaded. If that file is not found the internal version of the `us.kbm` keyboard mapping file is used.
`FHWEB-CLIENT_KBD_FILE_ROOT`	Specifies the root path name to the keyboard mapping files. The `kbd` directory that contains the keyboard mapping files is expected to be in this directory. **Example:** On Linux, `FHWEB-CLIENT_KBD_FILE_ROOT=/home/someuser` causes the file `/home/someuser/kbd/xxx.kbm` to be loaded, where `xxx` indicates the `LAYOUT` obtained from the following `FHWEB-CLIENT _KBD_FILE_LAYOUT` environment variable or automatically from the OS.
`FHWEB-CLIENT_KBD_LAYOUT`	Specifies which `LAYOUT` (or file name prefix) to use.

Environment Variable	Description
	This LAYOUT name, along with the appended .kbm extension, is used as the file name. **Example:** FHWEB-CLIENT_KBD_LAYOUT= MyCustomKeyMappingFile loads the file /ect/FH_Web/kbd/ MyCustomKeyMappingFile.kbm. If the above example for FHWEB-CLIENT_KBD_FILE_ ROOT is also used, the file /home/someuser/kbd/ MyCustomKeyMappingFile.kbm is loaded. A sub-directory of the root path name to the mapping files can also be included here. **Example:** FHWEB-CLIENT_KBD_LAYOUT=thinclient/us loads /etc/fhweb-client/kbd/ thinclient/us.kbm, provided a different root path is not specified. This will override the LAYOUT obtained automatically from the OS.

Note:

Previous versions of the Linux client use the command-line argument -kb and the plug-in/applet parameter keyboard to inform the server of the correct keyboard layout.

Example: -kb 0000040C overrides the environment variable LANG = en_US and causes the server to use the French keyboard layout.

This is no longer recommended. Each keyboard mapping file contains the correct keyboard layout value that the server should use. Specifying a different keyboard layout with the command-line argument -kb or the plug-in/applet parameter keyboard could cause the keys to operate in undefined ways.

The command-line argument -kb and the plug-in/applet parameter keyboard can still be used to load an IME by specifying a layout text.

Keyboard/IME identifiers used by FH Web Edition

FH Web Edition uses two identifiers, collectively known as FH Web Edition Input Identifiers (GGII), to specify a keyboard/IME for a session.

The first identifier is a keyboard layout. These are 8-digit string identifiers that Windows operating systems use to load keyboard drivers and IME programs. They are similar to locale IDs in that the last four digits typically match the 4-digit locale ID of the language supported by the keyboard. Keyboard layouts that specify an IME typically start with an "E". The list of available keyboard layouts can be viewed in the registry under the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts` key.

The second identifier used by FH Web Edition is the layout text string, which is a registry value of each keyboard layout registry key. These strings are displayed in the menu under **Keyboard layout/IME** when adding input languages.

In the following examples, the first example has a keyboard layout GGII of 00000409 and a layout text GGII of US. The second example has a keyboard layout GGII of E0010411 and a layout text GGII of Japanese Input System (MS-IME2002).

Example:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\00000409
Layout File = KBDUS.DLL
Layout Text = US
```

Example:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\E0010411
Ime File = imejp81.ime
Layout File = Kbdjpn.dll
Layout Text = Japanese Input System (MS-IME2002)
```

Configuring client keyboard options

You can specify the keyboard/IME for a session using the `-kb` shortcut parameter or the `keyboard` hyperlink parameter. These take both types of GGIIs described above. On Windows computers, if the `-kb` shortcut parameter is not specified, FH Web Edition uses the layout text of the currently active keyboard layout. On Linux computers, FH Web Edition does not send a layout text to the server if one is not specified on the command-line.

Example:

```
Windows shortcut using a keyboard layout:
FH_Web.exe -h server1 -kb 00000409
```

Specifying layout text substitutions

Layout text substitutions can be specified on the server to map between client and server keyboard layout names. These substitutions can be used to:

- Overcome differences in layout text names on different versions of Windows.
- Substitute an ANSI name for a keyboard layout that has a UNICODE name.

  Example: When specifying a keyboard layout with a UNICODE name through the `keyboard` applet parameter in an ASCII HTML page, it is necessary to substitute an ASCII name for the UNICODE name.

Keyboard layout substitutions are specified under the `HKEY_LOCAL_MACHINE\SOFTWARE\ACSXerox\FH Web Edition\System\Keyboard\Layout\Substitutes` registry key. Each REG_SZ value within this key has the name of a GGII, and the value is the name of a layout text from the server that should be used in place of the client name.

Setting fallback layout text

If there is no GGII specified from the client, or if the one specified fails to load a valid keyboard layout, the FH Web Edition server uses a fallback mechanism to determine which keyboard layout should be used for the session. The fallback layout text should be the layout text for the keyboard layout used by all clients connecting to the server, exclusive of those passing a valid GGII. The fallback layout text is automatically set during installation if the keyboard layout that is active is an IME. It may be modified after installation by editing the **Fallback Layout Text** value under the `HKEY_LOCAL_MACHINE\SOFTWARE\ACSXerox\FH Web Edition\System\Keyboard Layout` registry key.

Caution: When connecting to a Chinese FH Web Edition server, the **Sign In** dialog box appears from the shortcut along with the IME bar, specifying Chinese as the default language. Clicking CTRL+Spacebar does not toggle the languages. Users must manually click the IME bar with the mouse pointer to select English. Without manually clicking the IME bar, users are unable to type a user name and password.

Configuring multiple input locales

The default user account profile can be configured with different and/or multiple input locales. Account profiles for new users logging on to a FH Web Edition server are automatically configured with the default user account's input locales. Users can switch to any input locale that is defined in their account profile.

Note: Users with roaming profiles or profiles that already exist on the FH Web Edition server do not receive these new settings. These accounts must be configured manually.

Note: Users are not able to switch input locales when the **Sign In** dialog box is displayed. The input locale for the default language of the FH Web Edition server is used. On Windows clients, the selected input locale of server-based applications is not displayed in the system tray.

Administering user accounts

To access applications on a FH Web Edition server, clients must sign in to the server machine. When users start a FH Web Edition client, they are prompted for their user name, password, and the name of the server they wish to access. This information is optionally encrypted and passed to the Application Publishing Service running on the FH Web Edition server. The Application Publishing Service then performs the logon operation using standard multi-user features of Windows.

When a user signs in to a server and a domain is not specified, the FH Web Edition server first attempts to authenticate the account on the local machine, followed by the machine's domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name, followed by a backslash (\) and their network user name, in the **Sign In** dialog box, in **User name**.

Example: `NORTH\johng`

When a local user name on the FH Web Edition server is the same user name as a domain account, each with a different password, FH Web Edition treats them as two separate accounts.

Example: The following accounts and passwords exist:

- A local account on the FH Web Edition server `johng` with a password of `local`.
- A domain account `johng` with a password of `domain`.

When typing the user name `johng` with the password `local` in the **Sign In** dialog box, the account authenticates on the local FH Web Edition server. When typing `johng` with the password `domain` in the **Sign In** dialog box, FH Web Edition does not attempt to authenticate on the domain, but fails with an invalid user name or password. You must specify the domain name in the **User name** field in the **Sign In** dialog box as `NORTH\johng`.

Once a user is signed in, FH Web Edition relies on the server's operating system to provide the security necessary to run applications safely in a multi-user environment. Applications run in the security context of the client user to ensure private sessions. Access to all machines and network resources is governed by the operating system and the rights that have been granted to individual user's sessions.

Users must be able to log on interactively (locally) on the FH Web Edition server. Assign local logon rights to users in **Local Security Policy**, **Domain Security Policy**, and **Domain Controller Security Policy**.

This chapter contains basic information regarding on the FH Web Edition server. For more detailed information on the administration of user accounts, consult your Windows Help, accessible from the **Start** menu.

Setting up user profiles

Most Windows applications store user-specific settings and files under the user's Windows profile. By default, Windows creates a local profile for each user that logs on to a system. A local profile is specific to a given computer and does not work well if you are running multiple FH Web Edition servers.

If you are running a multiple-host environment, you should set up roaming user profiles. A roaming profile is stored centrally and can be accessed from any networked computer for which that profile is valid. When a user with a roaming profile logs on to any networked computer, the desktop appears exactly as the user left it the last time he or she logged off. For multiple-host environments, working with roaming profiles is the only way to ensure that user-specific settings are available to the user at all times.

Note:

- A profile is only valid on the platform for which it was created.

  Example: A Windows 7 profile can only be used on a Windows 7 computer.

Setting file permissions

As the system administrator, you may need to restrict user access to certain files and resources. Keep in mind that there are multiple users accessing the host. Particularly in a load-balanced server environment, we recommend write-protecting system and application folders so that users are unable to save files on a local FH Web Edition server. Otherwise, the next time a user logs on to FH Web Edition and is routed to a different server, the files and folders are inaccessible.

You must use Windows Explorer to set the permissions for files on the server. By setting file permissions, you can restrict user access to applications, printers, and folders. File permissions can only be set on drives formatted with the Windows NT file system (NTFS). If you are using the FAT file system, you are unable to set permissions for specific files or restrict access to applications.

Tip: While in Windows Explorer, choose the Help button or press F1 for more information on setting file permissions.

Setting up a network printer

As the administrator, you can set up network printers for use by FH Web Edition clients. You must first add a port on the FH Web Edition server that connects directly to the host, and then install the printer locally. This provides direct access to the printer.

1. Choose **Start** → **Settings** → **Printers**.
2. Double-click **Add Printer**.
3. Select local printer, and then click **Next**.
4. Click **Create a new port**, and then select **Standard TCP/IP Port** as the type.
5. Click **Next**.
6. In the **Port Name** dialog box, type the UNC path to the printer.

   Example: `\\PRINTSERVER\LASERPRINTER`, or the printer's IP address.

7. Do one of the following:
   - Select the printer manufacturer on the left and the printer model on the right,
   - Click **Have Disk**.
8. Follow the directions provided by the **Add Printer Wizard** to install the proper printer driver.

Web Edition Connection Manager

The FH Web Edition Connection Manager lets you administer, monitor, and control client access to the FH Web Edition server. The FH Web Edition Connection Manager displays a list of the users signed in to a FH Web Edition server, along with the applications the users are running, and the time the application was started. Through the FH Web Edition Connection Manager, you can perform a variety of administrative tasks, such as adding and removing applications, terminating user sessions, and ending processes running on the host.

Access the FH Web Edition Connection Manager

1. Do one of the following.
   - On your desktop, double-click the **FH Web Edition Connection Manager** icon.
   - Choose **Start → Programs → FH Web Edition Server → FH Web Edition Connection Manager**.

   The left pane of the FH Web Edition Connection Manager lists the hosts on the network running the Application Publishing Service. By default, the FH Web Edition Connection Manager displays information for the host running on your machine. To connect to other hosts and view information about them, click the host name from the list of FH Web Edition servers. If a host's icon has a red X, the administrator does not have administrative rights on the host.

   If the host's icon has a red X and is grayed out, the host is no longer running the Application Publishing Service, or it has been turned off. In either case, the administrator is unable to access that host from the FH Web Edition Connection Manager.

   In the left panel of the FH Web Edition Connection Manager, click the **All Hosts** icon to view a list of all active sessions on the network. This lets you view active FH Web Edition sessions without connecting to individual hosts. This is also helpful for locating a particular session's host.

   > **Note:** You must belong to the Administrators group on each FH Web Edition server to access that host from the FH Web Edition Connection Manager. Without administrative rights on a host, you are unable to add applications, terminate processes, etc.

Managing applications

For clients to run an application via FH Web Edition, the application must be added to the FH Web Edition Connection Manager. Clients are then able to connect to the FH Web Edition server and access the application.

Installing the application

FH Web requires an `.INI` type installation (not a registry installation) of **FIREHOUSE** Software® Enterprise Edition. Please refer to the ***FIREHOUSE*** *Software Enterprise Installation Guide* for specifics. We recommend contacting FH technical support to schedule your installation.

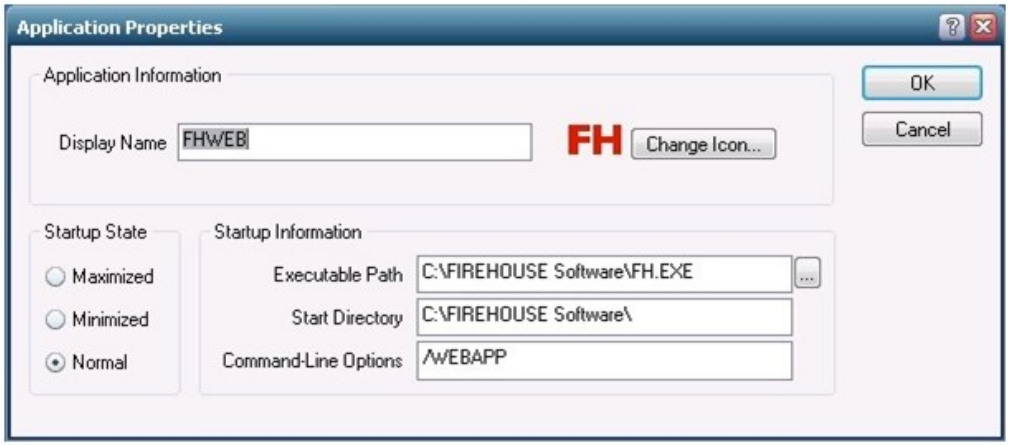
Adding applications

Applications must be added to the FH Web Edition Connection Manager before users can access them. When adding applications to the FH Web Edition Connection Manager, you can specify start-up parameters that control how the application opens and what processes are initiated when the application starts.

The **FIREHOUSE** Software executable (`FH.exe`) must be added to the FH Web Edition Connection Manager before users can access them. When adding `FH.exe` to the FH Web Edition Connection Manager , you also need to add the startup parameter of `/WEBAPP` to control how the application opens and what processes initiate when the application starts.

1. From **All Hosts**, select the host you want to add an application to.
2. Click the **Applications** tab.
3. Click **Add**.
4. Under **Application Information**, in **Display Name**, type `FHWEB`.
5. (Optional) Click **Change Icon** and select an icon other than the application's default icon.
6. Under **Startup State**, select the option indicating whether the application starts in a maximized, minimized, or in normal mode.
7. Under **Startup Information**, in **Executable Path**, type the path to `FH.EXE`, or click the browse button and navigate to it.

   By default, this file is located in `C:\FIREHOUSE Software`. If you browsed to find `FH.EXE`, the path to the file in **Start Directory**.
8. (If the path to FH.EXE does not appear in **Start Directory**) In **Start Directory**, type the full path to the directory in which you want the application to start.
9. In **Command-Line Options**, type `/WEBAPP`.
10. Click **OK**.



After registering an application with the FH Web Edition Connection Manager, the application's name and path appear in **Installed Applications**. You can sort items in the list in

ascending or descending order by clicking the column's title. This is true for all lists in the FH Web Edition Connection Manager.

If you want to set up applications that use ODBC data sources, you must set up the ODBC drivers as system DSNs (data source names), for FH Web Edition clients to be able to access the data sources. For more information about data sources, consult the Windows ODBC Data Source Administrator online Help.

Due to access restrictions, the FH Web Edition Connection Manager cannot verify the validity of paths specified in UNC format (Example: `\\Machine Name\Folder Name\...`), or that reside on a mapped network drive. If the path in **Executable Path** or **Start Directory** of a published item involves a mapped drive or is specified with a UNC path, the FH Web Edition Connection Manager accepts the specified path regardless of whether or not it is valid. If the path is invalid, or if the client user does not have rights to access the specified executable file or folder, the published item does not appear in the Program Window.

To resolve the situation, select the item and click **Properties**. Try updating the item's **Executable Path** or its **Start Directory**. If the item has been uninstalled or moved to a new location, it does not appear in the FH Web Edition Connection Manager when the Application Publishing Service is restarted.

The FH Web Edition Connection Manager is unable to display group and user settings for any item's path specified in UNC format or that resides on a mapped drive. The following message is displayed in the FH Web Edition Connection Manager's Application Users/Groups window for any application or file where this applies: `User/Group settings not available`.

If an item that resides on a mapped drive but is not licensed for use with FH Web Edition is published in the FH Web Edition Connection Manager, the item's icon appears in the Program Window. However, the user is not able to open the item, and receives an error message when attempting to launch it.

Tip: Right-click an item in **Installed Applications** or **Application Users/Groups** to display shortcut menus of the most frequently used commands.

Editing application properties

Once an application is added to the FH Web Edition Connection Manager, you can edit the application's properties at any time.

Example: You can edit the application's startup state, the location of its executable file, or the folder from which you want the application to start.

1. Click the **Applications** tab.
2. From **Installed Applications**, select an application.
3. Click **Properties**.
4. Edit any of the values in the dialog box, as you did in **Adding applications**, on page 26.

Duplicating an application

Duplicating an application makes an exact copy of the selected registered application. This feature is useful if you want to make the same application available to different users or groups, but with variations.

Example: You may want to register one version of an application with command-line options to bypass the **Sign In** dialog box, and another version without command-line options that requires clients to sign in.

Note: When duplicating an application, you must specify a new display name.

1. From **Installed Applications**, select the application you would like to duplicate.
2. Do one of the following.
   - Click **Duplicate**.
   - Choose **Tools** → **Applications** → **Duplicate**.

Renaming an application

The display name that you assign to an application appears to the end user in the Program Window. You can change an application's display name at any time.

1. From **Installed Applications**, select the application you would like to rename.
2. Do one of the following.
   - Click **Rename**.
   - Choose **Tools** → **Applications** → **Rename**.

Removing applications

You can remove FH Web Edition-deployed applications through the FH Web Edition Connection Manager. Removing an application from the FH Web Edition Connection Manager does not uninstall it from the host; it only prevents FH Web Edition clients from accessing the application.

If you remove an installed application from the FH Web Edition Connection Manager while a user is running the application, the user's session is not interrupted. When the user exits that application, however, the application is no longer available, and the icon does not appear in the Program Window.

1. Click the **Applications** tab.
2. From **Installed Applications**, select the application(s) you want to remove.
3. Do one of the following.
   - Click **Remove**.
   - Choose **Tools** → **Applications** → **Remove**.

Assigning launch parameters to users or groups

The FH Web Edition Connection Manager lets you assign specific parameters for how an application runs for users or groups on the network or on local machines. The parameters set for a user or group apply each time that user or group launches the application.

Application launch parameters set for an individual take precedence over parameters set for a group or for an application. When a client launches an application through FH Web Edition, the Program Window first checks for launch parameters assigned to the individual user. If no parameters are assigned, it checks the list of groups the user belongs to, in the order the Program Window obtains them from the system. Otherwise, the Program Window looks for generic launch parameters assigned to the application.

Tip: Check the user's **About FH Web Edition** box to verify what group or groups the user is assigned to, and in what order the groups are listed in the system.

File permissions for users and groups are controlled by Windows NT file system (NTFS) security settings on the host. File permission are not set through the FH Web Edition Connection Manager. When you select an application **Installed Applications**, the **Application Users/Groups** list displays the user permissions specified for that file and/or application with NTFS. You can then edit the application's properties for specific users or groups.

Note: File permissions can only be set on drives formatted with NTFS. If you are using the FAT file system, you are not able to set permissions for specific files or restrict access to applications.

1. Click the **Applications** tab.
2. From **Installed Applications**, select an application.
3. From **Application Users/Groups**, select a user or group.
4. Click **Properties**.
5. Do any of the following:
   - In **Start Directory**, type the full path of the directory in which you want the application to start.
   - Under **Startup State**, select whether the application starts maximized, minimized, or in normal mode.
   - In **Command-Line Options**, type the command-line arguments you want to use when launching the application.

Managing sessions and processes

Administrators can encrypt and shadow sessions and terminate processes and sessions through the FH Web Edition Connection Manager.

Terminating a session

When terminating a user's session, all FH Web Edition-deployed applications that the user is running are terminated, and the user is logged off the FH Web Edition server.

1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to terminate.
3. Choose **Tools** → **Sessions** → **Terminate**.

Ending a process

A process is any action taking place on a FH Web Edition server that is initiated by a client.

Example: A client running an application is a process.

Each running application is assigned a unique name and process ID in the Windows Task Manager. These process names and IDs are duplicated in the FH Web Edition Connection Manager. Administrators can end any process from the FH Web Edition Connection Manager.

1. Click the **Processes** tab.
2. Select the process or processes you would like to end.
3. Click **Tools** → **Processes** → **Terminate**.

WARNING: Terminating a session or ending a process without giving users a chance to close their application can result in the loss of data.

Shadowing a session

Session shadowing lets multiple users view and control a single session and its applications. This allows technical support and system administrators to provide remote assistance to customers and users. Session shadowing may also be used for live collaboration.

Note: Only administrators can connect to running FH Web Edition sessions, but only with permission from the session's user.

1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to shadow.
3. Do one of the following.
   - From the **Sessions Name** column, right-click the session you would like to shadow.
   - Choose **Tools** → **Sessions** → **Connect**.

The **Connection Notice** dialog box appears for the session's user, listing the administrator's user name and prompting for permission to connect.

Connection Notice
GerryD is asking to connect to your session.
Do you want to allow GerryD to connect to your session and view your applications and data?
Yes
No

If the user clicks **Yes**, the connection is made immediately and the FH Web Edition client session opens in a new frame window. If the user clicks **No**, an error message appears for the host.

Session shadowing is also denied when the session is disconnected, when the session is about to be or is in the process of being shut down, or when the user fails to respond within one minute. Connection is also denied in the event of a FH Web Edition communication failure.

The **Sessions** tab of the FH Web Edition Connection Manager displays the number of clients connected to a session. Two or more in the **Connected Clients** column indicates that the session is being shadowed. Disconnected sessions have no connected clients. To disconnect from a session and end session shadowing, simply close the frame window where the session is displayed.

> **Note:** When a FH Web Edition session is being shadowed, the host's cursor remains on the client until that session is closed. It does not go away even when the session is no longer being shadowed.

Security options

Through the **Security** tab of the **Host Options** dialog box, administrators can select the transport mode of communication between clients and the FH Web Edition server, and can select the level of encryption for data transmitted between client and host. Administrators can also modify the host port setting and enable integrated Windows authentication and password caching.

Selecting SSL transport

FH Web Edition provides support for both Transmission Control Protocol (TCP) and Secure Socket Layer (SSL) as methods for communication between Windows and FH Web Edition servers. When selecting the SSL transport, an SSL Certificate file must be specified. SSL certificates are required to secure communication between FH Web Edition clients and servers. You can obtain a certificate from a trusted Certificate Authority (CA) such as Verisign or Thawte, or you can create your own certificate authority and then sign your server certificates from this authority. Wildcard SSL certificates are also supported.

Obtaining a trusted server certificate

To obtain a server certificate from a CA that is trusted by the client operating system, consult the documentation from the CA of your choice using the following information as a guide. The CA will require a Certificate Signing Request (CSR).

Generate a CSR

1. Download OpenSSL from OpenSSL for Windows at http://www.openssl.org/related/binaries.html.

   Note: You must install the full version of OpenSSL: `Win32OpenSSL-v0.9.8a.exe`

2. Install OpenSSL on the FH Web Edition server.
3. Choose **Start** → **Run**.
4. Type `cmd`, and then press **Enter** on your keyboard.
5. Type the following command to generate a private key for the server:

   OPENSSL_DIR`\bin\openssl genrsa -out server.key 1024`

   where *OPENSSL_DIR* is the path to the directory in which OpenSSL is installed.

   Example: `C:\OpenSSL`

6. Type the following command:

   OPENSSL_DIR`\bin\openssl req -new -key server.key -out server.csr`

   You are prompted for the attributes to be included in your certificate, as follows:

   Country Name: US
   State: your state
   Locality: your city
   Organization: your company name
   Organizational Unit: your department

Common Name: your server's name
E-mail Address: your e-mail address

Unless you are using a wildcard SSL Certificate, the **Common Name** must match the host name of the FH Web Edition server (the name that users will specify when connecting to the host). Any variation in the name will cause the client to issue a warning when connecting.

The output of the command is a file named `server.csr`, which can be sent to your CA. Since FH Web Edition's SSL implementation is based on the OpenSSL toolkit, the tools used are the same as those used in other OpenSSL-based products, such as the Apache `mod_ssl` package. Follow instructions provided by your CA for the `mod_ssl` package to obtain a certificate for your server.

When your CA sends you the signed server certificate file, save it as `server.crt`. Copy this file and the `server.key` file (generated in step 5 above) to a directory on the FH Web Edition server that can be accessed from the system account and accounts that belong to the administrator group, but that cannot be accessed from normal user accounts. Finally, select the signed certificate file in the FH Web Edition Connection Manager.

Select the server certificate

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click the **Security** tab.
3. In the **Transport** list, select **SSL**.
4. In **SSL Certificate**, type or browse to the path to the server's certificate file.

   Example: `server.crt`

5. Click **OK**.

Using an Intermediary SSL Certificate with FH Web Edition

When using an intermediary SSL certificate with FH Web Edition, you must concatenate your existing certificate with the intermediary certificate.

Example: Below is the Go Daddy intermediary certificate.

1. Locate the `.crt` and `.key` files used on the FH Web Edition server.
2. Download the Go Daddy intermediary certificate (`GODaddyCA.crt`).

   Note: This should have come with the original certificate purchase, but can also be located at https://certs.godaddy.com/Repository.go.

3. Concatenate your `.crt` and the intermediary `.crt` file by combining them into a third file with the command:

   ```
   copy test_server.crt+GODaddyCA.crt server.crt
   ```

4. Rename the `.key` file from step 1 to `server.key`, so that it matches the newly created `server.crt` file.
5. Copy these two files to a location on the FH Web Edition server, such as `c:\Data`.
6. Launch the FH Web Edition Connection Manager.
7. Choose **Tools** → **Host Options**.
8. Click the **Security** tab.
9. (If you have a high-encryption license) Change the transport to SSL and increase the encryption level to 256-bit AES.
10. Browse to the SSL certificate `c:\data\server.crt` and click OK.

    Note: You should not see an error message if the `.crt` and `.key` files have the same prefix.

11. Enable **Notify users when connections are secure** for testing purposes.
12. Click **OK**.
13. Start a FH Web Edition session from a different system.

Creating your own certificate authority

A certificate authority is a virtual organization that signs each of your server keys, letting the client assert that the server keys are authentic and have not been tampered with.

Sites with many FH Web Edition servers can create their own certificate authority,and then sign each server's certificate from this authority and install the certificate authority certificates onto each client. This prevents any warnings about untrusted authorities, without requiring the site to obtain a third-party certificate for each server.

There are many third-party applications and systems to assist in the creation and maintenance of a certificate authority that interoperates with the OpenSSL toolkit. These tools are able to generate signed server certificates for use with FH Web Edition without modification.

To establish the certificate authority, a CA key and self-signed certificate must be created. Once the CA certificate and key are created, import the CA certificate on the client device through the **Internet Options** dialog box. Finally, the server keys are signed using the CA certificate, which allows the client machines to recognize the authenticity of the signatures and allow connections to the server without warning the user about the trustworthiness of the CA.

Note: Nine files are created during this process: `ca.key`, `ca.csr`, `ca.crt`, `ca.cfg`, `ca.serial`, `server.cfg`, `server.key`, `server.crt`, and `server.csr`.

Import the trusted server certificate on a dependent host

Note: You need to add a policy in the Microsoft Management Console. This is only required when using a self-generated certificate.

1. On the dependent host, choose **Start** → **Run**.
2. In the **Open** dialog box, type `mmc`.
   The Microsoft Management Console appears.
3. Choose **Console** → **Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Certificates**, and then click **Add.**
6. In the **Certificate Snap-in** screen, select **Computer account**, and then click **Next**.
7. In the **Select Computer** screen, select **Local computer**, and then click **Finish**.
8. Close the **Add Standalone Snap-in** dialog box.
9. Return to the **Add/Remove Snap-in** dialog box, and then click **Certificates (Local Computer)**.
10. Click **OK**.
11. Under **Console Root**, expand **Certificates**.
12. In the left pane, select **Trusted Root Certification Authorities**.
13. In the right pane, right-click **Certificates** and then choose **All Tasks** → **Import**.
14. Browse for the `ca.cert` certificate.

Verify certificate filenames and location

The server key and certificate files (`server.key` and `server.crt`) must have the same base filename and be located in the same directory on the FH Web Edition server. Dependent hosts do not need SSL certificates, but their designated relay server must have a valid SSL certificate signed by a CA and recognized by the dependent hosts.

1. On the dependent host, right-click **My Computer**, and the choose **Explore**.
2. Browse to `\FH Web Edition\Programs`.
3. Double-click `FH_Web.exe`.
4. Enter the name of the relay server as it is specified in the FH Web Edition Connection Manager.

   If the relay server has a valid SSL certificate signed by a CA and recognized by the dependent host, the **Security Alert** dialog box does not appear. If it does appear, the dependent host can not connect to the relay server.

Creating a CA Key and Certificate

The first step to establishing a certificate authority (CA) is to generate an RSA private key.

WARNING: This key should be kept very secret, as any entity with access to this key can generate false certificates that would certify unknown hosts as trusted. It is vitally important to protect the integrity of your certificate authority.

1. Generate the CA key by typing the command:

   OPENSSL_DIR`\bin\openssl genrsa -out ca.key 1024`

   Your initial CA key is generated and placed in the file `ca.key`.
2. Generate the Certificate Signing Request (CSR) by typing the command:

   OPENSSL_DIR`\bin\openssl req -new -key ca.key -out ca.csr`

   This command prompts you for the information to be contained in the certificate. The prompts should be answered as:

Prompt	Response
Country Name:	Your two-letter country abbreviation
State or Province Name:	Your full state or province name
Locality Name:	Your city or town or suburb name
Organization Name:	The name of your organization or company
Organizational Unit Name:	The organizational name should be a representation of your CA's name
Common Name:	Either be a person responsible for the operation of the CA or a generic name representing the CA itself
Email Address:	An e-mail address that can be used to for concerns about certificates to someone responsible for the CA

Prompt	Response
A challenge password []:	[enter]
An optional company name []:	[enter]

Example:
Country Name (2 letter code) [AU]:`US`
State or Province Name (full name) [Some-State]:`Iowa`
Locality Name (e.g., city) []:`Urbandale`
Organization Name (e.g., company) [Internet Widgits Pty Ltd]:`FIREHOUSE Software Web`
Organizational Unit Name (e.g., section) []:`Xerox`
Common Name (e.g., YOUR name) []:`Xerox`
Email Address []:`hostmaster@www.firehousesoftware.com`
Please enter the following extra attributes to be sent with your certificate request:
A challenge password []:`[enter]`
An optional company name []:`[enter]`

3. Establish the CA certificate by creating a file named `ca.cfg` and adding the following information to it.

```
extensions = x509v3
[ x509v3 ]
subjectAltName = email:copy
basicConstraints = CA:true,pathlen:0
nsComment = "your company site CA"
nsCertType = sslCA
```

4. Sign your CA certificate by typing the commands:

   OPENSSL_DIR`\bin\openssl x509 -req -extfile ca.cfg -days 1825 -signkey ca.key -in ca.csr -out ca.crt`

   These commands create the certificate file, `ca.crt`, which is the certificate that needs to be imported into the certificate store on each client device. It is also needed to create a configuration file for signing server keys.

5. Create a file named `server.cfg` and adding the following information to it.

```
extensions = x509v3
[ x509v3 ]
subjectAltName = email:copy
nsComment = "Certificate signed by your company CA"
nsCertType = server
```

6. Create a file that stores the serial numbers of certificates signed by this CA by typing the command:

```
echo 01 > ca.serial
```

Creating and signing server keys

1. Create a new server key by typing the command:

   OPENSSL_DIR`\bin\openssl genrsa -out server.key 1024`

   A new server key is generated and placed in the `server.key` file.

2. Generate a Certificate Signing Request (CSR) for the server key by typing the command:

   OPENSSL_DIR`\bin\openssl req -new -key server.key -out server.csr`

   You are prompted for information about the server certificate that you are generating.

Prompt	Response
Country Name:	Your two-letter country abbreviation
State or Province Name:	Your full state or province name
Locality Name:	The city, town, or suburb where your organization is located
Organization Name:	Either a department name or some name representing this server
Organizational Unit Name:	Either a department name or some name representing this server
Common Name:	The name of this server (not of a person) as it should appear on the certificate. **Caution:** The Common Name must match the host name of the FH Web Edition server. Any variation in the name will cause the client to issue a warning when connecting.
Email Address:	The e-mail address of a party responsible for this server
A challenge password []:	[enter]
An optional company name []:	[enter]

Example:
Country Name (2 letter code) [AU]:`US`
State or Province Name (full name) [Some-State]:`Iowa`
Locality Name (e.g., city) []:`Dillon`
Organization Name (e.g., company) [Internet Widgits Pty Ltd]:`D. Campbell Fire Company`
Organizational Unit Name (e.g., section) []:`.Fire & EMS`
Common Name (e.g., YOUR name) []:`server`
Email Address []:`tferguson@dcfc.com`
Please enter the following extra attributes to be sent with your certificate request:
A challenge password []:`[enter]`
An optional company name []:`[enter]`

3. Sign the server's key with the CA's certificate by typing the command:

   OPENSSL_DIR`\bin\openssl x509 -req -extfile server.cfg -days 1825 -CA ca.crt -CAkey ca.key -CAserial ca.serial -in server.csr -out server.crt`

   Note: The `-days 1825` parameter causes our server certificates to expire in 1825 days, or roughly 5 years. If you want certificates to expire earlier or later, adjust this number to fit your requirements.

4. Copy the `ca.crt`, `server.key`, and `server.crt` files to a directory on the target server that can be accessed from the system account, but cannot be accessed from the accounts of users who sign in to the host.
5. Select the server certificate in the FH Web Edition Connection Manager.
   a. In FH Web Edition Connection Manager, choose **Tools→ Host Options**.
   b. Click the **Security** tab.
   c. In the **Transport** list, select **SSL**.
   d. Type or browse to the path to the server's certificate (`server.crt`) file in **SSL Certificate**.
   e. Click **OK**.

Notifying users of a secure connection

When the SSL transport is selected, you can notify users with a **Security Alert** dialog box when connections are secure. All connections to that FH Web Edition server use the SSL transport and the selected encryption algorithm, including connections from FH Web Edition Connection Managers, clients, and dependent hosts.

Security Alert
You have a secure connection to "support-server".
Any information you exchange with this site cannot be viewed by anyone else on the Web.
OK

1. In the FH Web Edition Connection Manager, choose **Tools → Host Options**.
2. Click the **Security** tab.
3. In the **Transport** list, select **SSL**.
4. Type or browse to the path of the server's certificate file in **SSL Certificate**.
5. Click **Notify users when connections are secure**.
6. Click **OK**.

Encrypting sessions

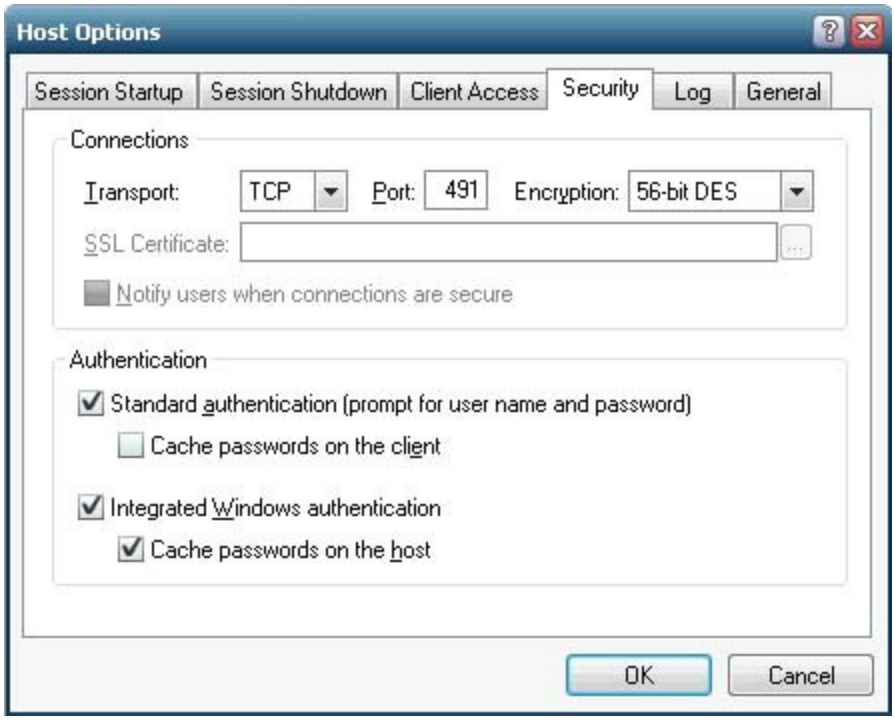
For purposes of security, administrators can choose to encrypt all data transmitted between the client and the host. This includes the client's user name and password, which are supplied during logon, and any application data submitted by the client or returned by the host.

When TCP transport mode is selected, FH Web Edition uses 56-bit DES encryption. The DES key is exchanged using RSA Public-Key Cryptography Standards. The RSA keys are 512-bits. When SSL transport mode is selected, the following encryption algorithms are also available: 128-bit RC4, 168-bit 3DES, and 256-bit AES.

> **Note:** A special license is required to use these algorithms. To obtain this license, contact your **FIREHOUSE** Software sales representative.

Once encryption is enabled, all succeeding FH Web Edition sessions are encrypted. Sessions that are active when the feature is enabled remain unencrypted. The next time the user signs into the FH Web Edition server, however, his or her session is encrypted. The user must sign off the FH Web Edition server, and sign back in for his or her session to be encrypted.

1. Choose **Tools** → **Host Options**.
2. Click the **Security** tab.



3. From **Encryption**, select an encryption level.
4. Click **OK**.

Modifying the host port setting

For users to access FH Web Edition through a firewall or router, administrators are able to modify the host port setting for the Application Publishing Service.

Caution: The Application Publishing Service must be running on a dedicated port. Conflicts may arise if another service is running on the same port. The default port number for both TCP and SSL is 491.

Note: After changing the host port, you must restart the Print Spooler Service and the FH Web Edition Application Publishing Service for client printing to work on a port other than the default port 491.

1. From the list of **All Hosts**, select the host you want .
2. Choose **Tools** → **Host Options**.
3. Click the **Security** tab.
4. In **Port**, type a new port number .
5. Click **OK**.

Note:

- Once you modify the host port setting, you need to modify the port parameter from the FH Web Edition hyperlink. Use the port parameter followed by the new port number.

  Example: `http://hostname/fhweb/logon.html?port=1667`

- Users running FH Web Edition from a shortcut need to append the `-hp` argument, followed by the new port number, to the shortcut.

  Example: `"C:\Program Files\ACSXerox\FH Web Edition\Client\FH_Web.exe" -h server1 -hp 1667`

- Users can also specify the port number in the Connection dialog when signing in to FH Web Edition. In the **Host Address** box, type the host name or IP address, followed by a colon and the port number.

  Example: `server1:1667>`

- If it is an IPv6 address, the IP address of the host must be in brackets.

  Example: `[fe80::29c:29ff:fe95:519a]:491`

- If the new port number is not specified by either of these methods, users are unable to sign in to FH Web Edition.

Standard authentication

Standard authentication is the default method for authenticating users on a FH Web Edition server. Standard authentication lets users sign in to FH Web Edition through the **Sign In** dialog box by supplying their user name and password. Once authenticated, users are added to the host's INTERACTIVE group and given the same access rights as if they had signed in to the host at its console.

1. Choose **Tools** → **Host Options**.
2. Click the **Security** tab.
3. Click **Standard authentication (prompt for user name and password)**.
4. Click **OK**.

Integrated Windows authentication

Integrated Windows authentication allows users to connect to a FH Web Edition server and start a session without having to sign in to the host and re-enter their user name and password. When Integrated Windows authentication is the only option enabled, the user's user name and password are never transmitted over the network. Instead, FH Web Edition runs the user's session in the same security context as the FH Web Edition client. Users are added to the host's NETWORK group instead of its INTERACTIVE group. As a result, they may be denied access to some resources.

When users connect to a FH Web Edition server using Integrated Windows authentication, they are able to access most of the same resources on the host that they would be able to access if they signed in to the host interactively. However, depending on the authentication protocols supported by the client's and host's operating systems and the network, when users access resources that reside on other computers on the network, they might be required to re-enter their user name and password. If network resources are unable to request a user name and password, access might be denied.

To access other computers on the network, Active Directory must be configured to allow authentication credentials to be passed to other computers. Microsoft refers to the right to pass authentication credentials to a third or more computers as "delegation." Delegation is supported by Windows 2000 or later on Active Directory networks with the proper settings. Instructions on properly configuring an Active Directory Domain Controller is available in your Microsoft Windows operating system documentation .

Windows NT domains do not support delegation. When Integrated Windows authentication is enabled in this environment, users might not have access to resources that reside on other computers on the network. To avoid these resource access limitations, **Configuration requirements for delegation support**, on page 82.

Note: The cache passwords on the host option, described in the following section, can be enabled to obtain an INTERACTIVE group logon with Integrated Windows authentication.

Caution: Integrated Windows authentication is only available to users who sign in from Windows computers that are members of the same domain as the FH Web Edition server.

Enable integrated Windows authentication

1. Choose **Tools** → **Host Options**.
2. Click the **Security** tab.
3. Enable **Integrated Windows authentication**.
4. Click **OK**.

   FH Web Edition requires that you select either **Standard authentication** or **Integrated Windows authentication**. If neither one of these authentication methods is selected and you click **OK**, an error message appears.

   If both **Standard authentication** and **Integrated Windows authentication** are selected, the FH Web Edition server will first attempts to log the user on with Integrated Windows authentication. If this fails, FH Web Edition then attempts to log the user on with standard authentication by presenting the **Sign In** dialog box and requiring a user name and password.

Password caching on the host

When a user signs in to a FH Web Edition server with standard authentication (either with a user name and password supplied by the **Sign In** dialog box, parameters, or command-line arguments), that user is added to the host's INTERACTIVE group. A user that signs in to a FH Web Edition server using Integrated Windows authentication is added to the host's NETWORK group. By default, members of the INTERACTIVE group have greater access to the host's resources than members of the NETWORK group. As a result, a user that signs in with Integrated Windows authentication may encounter "access denied" errors under a number of conditions.

Note: Areas restricted from members of the NETWORK group include DCOM (also known as OLE and COM/COM+) security limitations, file security limitations, and application specific security checking. Administrators should verify that all resources (files, services, etc.) that integrated Windows authenticated users need to access have the proper security settings to allow that access.

To avoid these errors, administrators can enable the cache passwords on the host option. Doing so allows users to sign in from Windows computers that are members of the same domain as the FH Web Edition server, without having to enter their user name and password every time they connect.

Users are prompted for a password when first connecting to the host or following a password change. Passwords are stored within their respective profiles and can only be decrypted from within their respective security contexts. With subsequent connections to FH Web Edition, users are automatically signed in and added to the host's INTERACTIVE group. They are granted the same access rights had they signed in to the host at its console.

Caching passwords on the host requires delegation, which is supported by Windows 2000 or later on Active Directory networks with the proper settings. Instructions on properly configuring an Active Directory Domain Controller are available in your Microsoft Windows operating system documentation. For a list of configuration requirements for delegation, see Configuration Requirements for Delegation Support in Chapter 6.

Enable password caching on the host

1. From the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click the **Security** tab.
3. Enable **Integrated Windows authentication**.
4. Enable **Cache passwords on the host**.
5. Click **OK**.

   FH Web Edition caches passwords on the host using industry standard encryption algorithms, provided by Microsoft's Data Protection application programming interface (DPAPI). For more information about DPAPI, search the MSDN Library (http://msdn.microsoft.com/library/default.asp) for "Windows Data Protection."

Password caching on the client

Client-side password caching is supported on all FH Web Edition clients. Client-side password caching allows users who are not members of the FH Web Edition server's domain to sign in to FH Web Edition without having to enter their user name and password every time they connect to the server. When cache password on the client is enabled, the **Sign In** dialog box includes a **Remember me on this computer** option. If the user selects this, after the first manual authentication, the user's logon credentials are encrypted on the host using the SYSTEM account context, transmitted over the network, and stored on client computers in user-private directories.

When the user makes subsequent connections to the server, the cached password is transmitted back to the host, where it is decrypted using the SYSTEM account context. The **Sign In** dialog box is displayed with the user name and password and with **Remember me on this computer** selected. If the user disables **Remember me on this computer**, the user's credentials are deleted from the client computer.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click the **Security** tab.
3. Enable **Standard authentication (prompt user for user name and password)**.
4. Enable **Cache passwords on the client**.
5. Click **OK**.

   On most platforms, the cached password is stored in the user's home directory in a `.dat` file named for the FH Web Edition server. With the Windows CE Client, the cached password is stored in the user's registry settings. The table below provides example locations of the cached password for each FH Web Edition client.

   Example: `user1` is the user name, `server1` is the name of the FH Web Edition server, and `192.168.100.111` is the IP address of the FH Web Edition server.

Platform	Password locations
Mac OS X	`/Users/user1/.fhweb-client/192.168.100.111.dat`
Windows	`C:\Documents and Settings\user1\Application Data\ACSXerox\FH Web Edition\server1.dat`

Platform	Password locations
Linux	`/home/user1/.fhweb-client/192.168.100.111.dat`
Windows CE	In the registry: `HKEY_CURRENT_USER\\Software\\ACSXerox\\FH Web Edition\\Client\CachedPasswordServers\\SERVERNAME`

Password change

Users can change passwords when:

- The administrator requires the user to change his or her password at the next logon.
- The security policy prompts users to change passwords before expiration.
- The user's password has expired.

Changing passwords at the next logon

Administrators can require a user to change his or her password by selecting **User must change password at next logon** in the **Administrator Properties** dialog box. (For local accounts, this dialog box can be accessed by choosing **My Computer** → **Manage** → **Local Users and Groups** → **Users** → **UserName** → **Properties**).

1. Access the FH Web Edition client installation file (http://hostname/fhweb/clients.html) (http://host/fhweb/clients.html) and select a FH Web Edition client.
2. Type the user name and password in the **Sign In** dialog box.

   Note: If the client account does not exist in the domain in which the FH Web Edition server resides, include the domain name in **User name** as a prefix.

   Example: `domain\username`
3. Click **OK**.

   The message "You are required to change your password at first logon" appears.
4. Click **OK**.
5. In the **Change password** dialog box, in the **New Password** and **Confirm New Password**, type a new password.
6. Click **OK**.

Changing a password before expiration

By default, users are prompted to change their passwords whenever they log on within 14 days of their password's scheduled date of expiration. Administrators can modify the change password prompt period by editing the prompt user to change password security setting.

Example: The local security setting can be viewed and changed by clicking **Start** → **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Local Policies** → **Security Option**.

You can log on during the password change prompt period.

1. Access the FH Web Edition client installation file (http://host/fhweb/clients.html) and select a FH Web Edition client.
2. Type the user name and password in the **Sign In** dialog box.
3. Click **OK**.

   The following message appears:

   ```
   Your password will expire in x day(s). Do you want to change your password now?
   ```

4. Click **Yes** or **No**.

   If you click **No**, the FH Web Edition session starts. If you click **Yes**, the **Change Password** dialog box appears.

5. In **New Password** and **Confirm New Password**, type a new password .

Changing a password after expiration

1. Access the FH Web Edition client installation file (http://host/FH_Web_Edition/clients.html) and select the appropriate FH Web Edition client.
2. Type the user name and password in the **Sign In** dialog box.

   Note: If the client account does not exist in the domain in which the FH Web Edition server resides, include the domain name in **User name** as a prefix.

   Example: `domain\username`

3. Click **OK**.

   The message “Your password has expired and must be changed” appears.

4. Click **OK**.
5. In the **Change password** dialog box, in the **New Password** and **Confirm New Password**, type a new password.
6. Click **OK**.

Password change and Integrated Windows authentication

When **Integrated Windows Authentication** is selected, FH Web Edition relies on the operating system of the client to change passwords.

Example: FH Web Edition supports the following scenario:

1. The administrator edits a user's settings and selects **User must change password at next logon**.

   The user is prompted to change his or her password the next time they log in.

2. The user changes the password and signs in to the client computer.

3. The user starts the FH Web Edition client and connects to a FH Web Edition server.

   The password has already been changed, so the user is authenticated on the host without being prompted for a password, unless the cache passwords on the host option is enabled. In this case, the user is prompted to enter a new password.

   If, however, the administrator selects **User must change password at next logon** after the user has logged on to the client computer, and the user subsequently connects to a FH Web Edition server that has Integrated Windows authentication enabled, authentication may fail. If it fails and both **Integrated Windows Authentication** and **Cache passwords on the host** are enabled, the user is prompted to sign in and make a password change.

Tip: In the FH Web Edition Connection Manager's dialog boxes, you can access Help by right-clicking an item, and then choosing **What's This?**. A pop-up window appears, containing a brief explanation of the item. You can also access Help by clicking the Help icon on the title bar of a dialog box, and then selecting an item.

Shared account

A shared account should be specified when multiple users are using the same account for starting a FH Web Edition session. Users who sign in to FH Web Edition with a shared account cannot disconnect and then reconnect to FH Web Edition. This prevents a user from reconnecting to another user's session. When logging on to a FH Web Edition server with a shared account, the user's session terminates immediately after disconnecting from the host, regardless of the reconnect setting in the FH Web Edition Connection Manager.

If an administrator designates an existing user name as a shared account while that user is disconnected from his or her session, the session remains running on the server until the termination limit is reached. The session is then terminated.

Note: Before specifying a shared account, verify in the FH Web Edition Connection Manager that there are no connected or disconnected sessions using that account.

FH Web Edition does not support the use of domain names for shared accounts, such as `NORTH\-johng`.

Note: FH Web Edition supports only one shared account per host.

1. Choose **Tools** → **Host Options**.
2. Click the **General** tab.
3. In **Shared account**, type the user name of the shared account.
4. Click **OK**.

Session reconnect

Session reconnect allows sessions to be maintained on a FH Web Edition server without a client connection. If the client's connection to the host is lost, intentionally or unintentionally, the user's session and applications remain running on the FH Web Edition server for the length of the session timeout specified in the FH Web Edition Connection Manager. Session reconnect allows users to return to their FH Web Edition session in the exact state they left it. Through the Program Window, users can select to disconnect, rather than exit from FH Web Edition, and can return to their session as they left it—without having to shut down their open applications and running processes.

If the network connection is lost or if users unintentionally disconnect from FH Web Edition, their session state is preserved for the length of time specified in the FH Web Edition Connection Manager. After a user is authenticated through normal logon procedures, FH Web Edition determines if the user has an active session. If so, that session resumes and appears exactly as it did prior to disconnection. If not, a new session is started. Users are also able to disconnect from one client and reconnect to the session from another client.

When attempting to reconnect to a disconnected session, users are required to specify their logon credentials. After the host validates them, the host reconnects them to the disconnected session. If the session is hosted on a server that is part of a load-balanced configuration, the user is routed to his or her session without any indication that the session is on a load-balanced server. If Integrated Windows authentication is available, users are automatically re-authenticated and re-connected to their session.

Setting the session termination

Administrators control how long client sessions and applications remain running on the FH Web Edition server through the FH Web Edition Connection Manager's **Host Options** dialog box.

The **Sessions** tab of the FH Web Edition Connection Manager displays the number of clients connected to a session. Disconnected sessions have 0 connected clients.

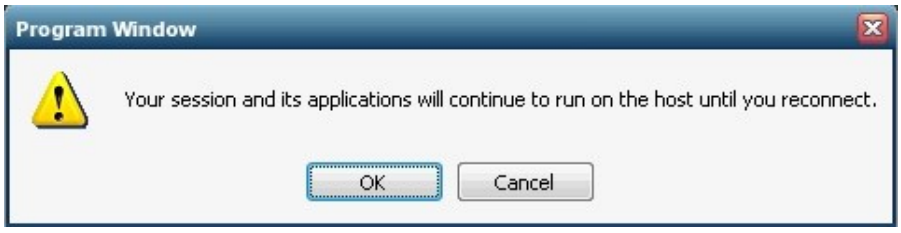
1. From the FH Web Edition Connection Manager, click **Tools** → **Host Options**.
2. Click the **Session Shutdown** tab.
3. Enable **Disconnected sessions terminate**.
4. Select one of the following session termination options:
   - **Immediately**, to terminate client sessions as soon as the client disconnects. This is the default setting.
   - **Never**, to terminate sessions only when a user manually closes all applications running within a session or when an administrator manually terminates a session using the FH Web Edition Connection Manager.
   - **After __ minutes** to specify the number of minutes a session remains running after a client disconnects from the session. Type the number of minutes in the edit field that a session should remain running after the client disconnects.
5. Click **OK**.

Disconnecting a session

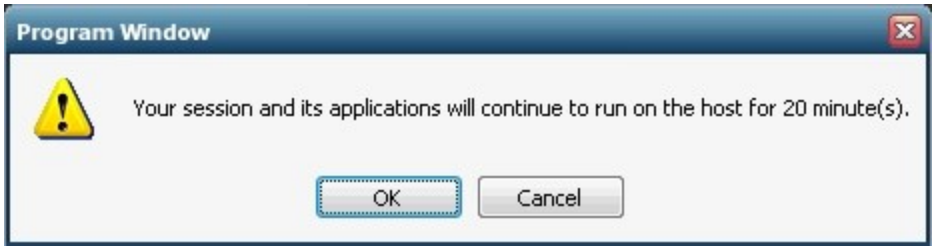
If sessions are set to never terminate or to terminate after a specified number of minutes, the Program Window's File menu includes a Disconnect option. If sessions are set to terminate immediately, the Disconnect option does not appear in the Program Window's File menu.

- In the Program Window, choose **File** → **Disconnect**.

  With session termination set to Never, the following message is presented to the user upon disconnecting from FH Web Edition:



  When sessions are set to terminate after a specified number of minutes (Example: 20 minutes) a message such as the following is presented to the user upon disconnecting from FH Web Edition:



  If a user attempts to disconnect from a session and already has a disconnected session, the following message appears:

  ```
  You already have a session (session_name) that is disconnected. If you disconnect the current session, that previous session will be terminated. Do you want to continue?
  ```

  If the user clicks **Yes**, the disconnected session is terminated. If the user clicks **No**, the user is returned to the running session.

> **Note:** When a user reconnects to a session, the command-line arguments -a, -r, and -ac are ignored.

Client time zone

By default, all FH Web Edition sessions are run in the time zone of the FH Web Edition server machine. Administrators can opt to run FH Web Edition sessions in the time zone of the client computer in the FH Web Edition Connection Manager.

1. Choose **Tools** → **Host Options**.
2. Click the **General** tab.
3. Select **Use client's time zone**.
4. Click **OK**.

Monitoring host activity

The FH Web Edition Connection Manager displays information about host activity and processes taking place on the host. Administrators can use this information to make decisions, such as determining which applications are no longer being used and whether additional hosts are required.

Viewing session information

- In the FH Web Edition Connection Manager, click the **Sessions** tab.

  The following session information is displayed.

Column	Displays the
Session Name	Unique identifier assigned to a session.
User	Network user name of the user accessing applications on the host.
Connected Clients	Number of clients connected to a session. 0 indicates that no one is connected to the session (the client has disconnected). 1 indicates that the client is connected and the session is active. 2 or higher indicates that the session is being shadowed.
IP Address	IP address of the client computer from which the user is accessing the host. (Each computer on a network has a unique IP address.)
Startup Time	Date and time the user started the application.
Applications	Number of applications the user is accessing.

Viewing process information

- In the FH Web Edition Connection Manager, click the **Processes** tab.

  The following session information is displayed.

Column	Displays the
Name	Name of the application running on the host.
User	Network user name of the user accessing the application.
Startup time	Date and time the user started the application.
Process ID	Process identification number assigned by the host's operating system. (The number for each running application matches the process identification number displayed in the Windows Task Manager.)

Displaying the status bar

The status bar appears at the bottom of the FH Web Edition Connection Manager window and provides brief descriptions of menu commands when the mouse pointer is placed over that item in the menu. The status bar indicates:

- The name of the FH Web Edition server currently being accessed.
- The memory usage and CPU utilization for that host, as calculated by the Windows Task Manager.
- The number of sessions running on the active FH Web Edition server.
- The number of processes running on the active FH Web Edition server.

Note: If **All Hosts** is selected, the sessions number reflects all the sessions running on the network, and the processes number reflects all the processes on the network.

You can choose whether or not to display the status bar.

1. Choose **View** → **Options**.
2. Select or clear **Status Bar**.

Setting the broadcast interval

You can modify how often host information is sent to the FH Web Edition Connection Manager by modifying the broadcast interval value. This value represents how many seconds elapse between broadcasts, affecting how often a host's CPU, memory, sessions, and process status bars are updated, and how long it takes a host to appear in the list of all hosts. The broadcast is sent through UDP and has a packet size of approximately 25-37 bytes.

1. Navigate to `C:\ProgramData\ACSXerox`, open the `HostProperties.xml` file in Wordpad, and locate the following section:

```
</property>
<property id="BroadcastInterval" group="Miscellaneous" type-
e="UINT32">
<value>10</value>
</property>
```

2. Type the desired number of seconds for the value.

   Note: This value must be an integer greater-than or equal-to 1. Setting the value to 0 prevents other FH Web Edition servers from being listed in the FH Web Edition Connection Manager. The default value for broadcast interval is 10.

3. Stop and start the FH Web Edition Application Publishing Service.

Session startup options

Administrators can enable startup options to control group policies, progress messages, and logon scripts. Administrators can also set various resource limits.

Applying group policy

FH Web Edition supports Microsoft's Group Policy. Using Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options.

Information on this features is available in Group Policy, at http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx.

1. From the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Session Startup**.
3. Select **Apply Group Policy**.
4. Click **OK**.

> **Note:** It may take users longer to sign in to FH Web Edition when **Group Policy** is enabled.

Displaying progress messages

After a user is authenticated, a dialog box that reports session startup progress can be displayed to users. When enabled, these messages inform users:

- When their personal setting are loaded.
- When group policy is applied.
- When network drives are connected.
- When logon scripts are run.

You can choose whether or not to display session startup progress messages to users.

1. From the FH Web Edition Connection Manager, click **Tools** → **Host Options**.
2. Click **Session Startup**.
3. Select **Display progress messages**.
4. Select **Always in front** to ensure that messages are displayed in front of all other windows.

> **Note:** If a logon script has the ability to display user interface to the user, **Always in front** option should be cleared, or the logon script's user interface may be partially obscured by the progress message.

5. Click **OK**.

Logon scripts

Logon scripts let administrators configure the operating environment for FH Web Edition users. Scripts may perform an arbitrary set of tasks such as defining user-specific environment variables and drive letter mappings.

FH Web Edition supports two types of logon scripts:

- Global scripts that execute for all users that sign in to the host.
- User-specific scripts that execute for individual users.

Before loading the user's profile and launching the Program Window, FH Web Edition's Logon Manager checks to see if a script of either (or both) type has been specified. If so, the Logon Manager runs the script(s) within the user's security context each time the user is authenticated.

User-specific logon scripts are specified using the functionality provided by the operating system.

Running logon scripts

Caution: Authenticated users must have read and execute access to the logon script files.

Note: Microsoft's VBScripts are not supported as logon scripts unless they are run in a batch file.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Session Startup**.
3. Depending on the type of script you want to run, do one of the following.
   - Select **User-specific**.
   - Select **Global**, and then specify the path of the global script file.
4. Click **OK**.

   If a logon script fails to execute, an error appears.

   Tip: When such an error occurs, check the location of the logon script.

   - If the user's account is a domain account:
     - `\\`*pdcname*`\NETLOGON` (the NETLOGON share of the primary domain controller)
     - `\\`*pdcname*`\SYSVOL\domainname`, (the domain subdirectory of the primary domain controller's SYSVOL share)
   - If the user's account is a local account:
     - *systemroot*`\System32\Repl\Import\Scripts`
     - *systemroot*`\sysvol\sysvol\`*domainname*

   Additional tools are available from DebugView for Windows v4.76, at http://www.microsoft.com/technet/sysinternals/utilities/DebugView.mspx, and can help track the cause of the problem when these errors occur. Open the DebugView executable on the host and check for any errors that point to the incorrect location of the script.

Setting resource limits

FH Web Edition lets administrators prevent users from starting new sessions when certain resource limits are exceeded on a FH Web Edition server. These limits help administrators prevent hosts from becoming loaded to the point where users experience performance problems and random resource allocation failures.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Session Startup**.
3. Select **Maximum sessions per user** and then enter the maximum number of sessions per user.
4. Click **OK**.

Specifying the maximum number of sessions

By default, the maximum number of sessions that can be supported from a given host is set to 50. Administrators should adjust this value to one that is appropriate for the capacity of the host.

1. From the list of hosts, select the host you want.
2. Choose **Tools** → **Host Options**.
3. Click the **Session Startup** tab.
4. In **Maximum sessions on this host**, enter an appropriate value.

   This value sets the limit for the number of sessions the host can support.

   Example: If the maximum number of sessions is 11, the user who initiates the twelfth session is prevented from logging on.

   In a relay server setting, FH Web Edition checks the maximum sessions setting on the relay server and its dependent hosts. The **Maximum sessions on this host** value designated on the relay server is the maximum number of sessions that can be run concurrently on all dependent hosts assigned to that relay server.
5. Click **OK**.

Specifying the minimum physical and virtual memory

You can prevent users from logging on when there is not enough physical or virtual memory on a host.

To prevent users from logging on when	Select this
Physical memory on a host falls below a given value	In **Minimum available physical memory**, enter a value.
Virtual memory on a host falls below a given value	In **Minimum available virtual memory**, enter a value.

Session shutdown options

Through the FH Web Edition Connection Manager, administrators can specify time limits for the number of minutes of client idle time, and the number of minutes that sessions are allowed to run on a host. Administrators can also specify whether the user is either disconnected or logged off when the idle limit is reached, and when to display warning messages to users about to be disconnected or logged off. Administrators can also designate a grace period during the log off period to let users save files and close applications.

Specifying the session limit

The session limit is the number of minutes that a session is allowed to run on a FH Web Edition server. The minimum amount of session time is one minute, and the maximum is 44640 minutes (31 days). This feature is disabled by default.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click the **Session Shutdown** tab.
3. Select **Session**, and then type the number of minutes that a session is allowed to run on a host before its user is logged off.
4. Click **OK**.

Specifying the idle limit

Idle time is the number of minutes since the last mouse or keyboard input event was received in a session. The idle limit is the number of minutes of idle time that a FH Web Edition server allows. The minimum amount of session time is one minute, and the maximum is 44640 minutes (31 days). This feature is disabled by default.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click the **Session Shutdown** tab.
3. Select **Idle**, and then type the number of minutes of idle time allowed by the host.
4. From the **Action** list, select **Disconnect** to disconnect users when the idle limit is reached, or select **Log off** to log users off when the idle limit is reached.
5. Click **OK**.

Specifying the warning period

The warning period is the number of minutes before a session limit or idle limit is reached, when users are warned they are about to be disconnected or logged off.

Example: If the warning period is set to `2`, users are warned 2 minutes before the session limit or the idle limit is reached.

This feature is disabled by default.

Caution: The warning period must be less than the session limit and idle limit settings.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Session Shutdown**.
3. Select **Warning period**, and then type the number of minutes before a session or idle limit is reached, when users are warned that they are about to be disconnected or logged off.
4. Click **OK**.

Specifying the grace period

The grace period is the number of minutes after an automated logoff begins, during which users may save files, close applications, and so forth. The session or idle limit determines when an automated logoff begins. The minimum grace period value is one minute, and the maximum value is 15 minutes. By default there is no grace period.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Session Shutdown**.
3. Select **Grace period**, and then specify the number of minutes after a logoff begins that users are able to save files and close applications,and so forth.
4. Click **OK**.

Managing FH Web Edition servers from client machines

Administrators can connect to the FH Web Edition Connection Manager from any client machine. This lets the administrator end processes, terminate sessions, and administer applications from any machine running a FH Web Edition client.

1. Set the permissions for the FH Web Edition Connection Manager so that only FH Web Edition administrators can access the application.
2. In Windows Explorer, locate the FH Web Edition`\Programs\cm.exe` file.
3. Right-click `cm.exe` and select **Properties**.
4. In the **Properties** dialog box, select **Security**.
5. In the **Security** dialog box, select **Permissions**.
6. In the **File Permission** dialog box, set the permissions so that only FH Web Edition administrators can execute the application.

   Tip: For help with setting permissions in Windows Explorer, click the **Help** button in the **File Permission** dialog box, or press F1 on your keyboard while running Explorer.
7. Add the FH Web Edition Connection Manager (`cm.exe`) as a registered application with the FH Web Edition Connection Manager.
8. From the client machine, log on to a FH Web Edition server as a FH Web Edition administrator, or as a user with administrative rights on the host.

   This will launch the Program Window.
9. From the Program Window, launch the FH Web Edition Connection Manager by clicking the **FH Web Edition Connection Manager** icon.

   This icon appears in the Program Window only if the user has administrative rights on the host. You can administer applications and user access as if running the FH Web Edition Connection Manager from the FH Web Edition server.

Keyboard shortcuts for the FH Web Edition Connection Manager

Applications tab

Action	Result
Double-click the application	Displays the **Application Properties** dialog box.
DELETE*	Removes the selected application.
CTRL+A*	Displays the **Application Properties** dialog box.
CTRL+S	Displays the **Application Properties for Users/Groups** dialog box.

Sessions tab

Action	Result
DELETE	Terminates the selected session.

Processes tab

Action	Result
DELETE	Terminates the selected process.

General

Action	Result
CTRL+TAB	Cycles through tabs.
CTRL+SHIFT+TAB	Reverse cycles through tabs.
CTRL+P	Displays the **Options** dialog box.
CTRL+B	Displays or hides the status bar.
ALT+F4	Exits the FH Web Edition Connection Manager.
F1	Displays Help for the FH Web Edition Connection Manager.
F5	Refreshes the **Sessions**, **Processes**, and **Applications** tabs.
INSERT	Displays the **Add Application** dialog box.

*An application from **Installed Applications** must be selected for these shortcuts to work.

Running FH Web Edition

FH Web Edition can be run from a Web browser or from a computer's desktop.

Running FH Web Edition from a web browser

FH Web Edition can be run from popular Web browsers, including Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

1. Start a Web browser.
2. In **Location** , type `http://`, followed by the host name and the FH Web Edition logon page.

   Example: `http://hostname/fhweb/logon.html`

3. Follow the on-screen instructions that prompt you to install a FH Web Edition add-on for your browser.
4. In the **Sign In** dialog box, type the network user name and password.

   Note: FH Web Edition allows users three invalid logon attempts before shutting down the logon process.

Running FH Web Edition from a computer's desktop

To run FH Web Edition from the desktop of a computer, you must first install the FH Web Edition client, and then launch it from the computer's start menu, a shortcut, or a console window.

Install the FH Web Edition client

1. Start a Web browser such as Safari, Firefox, or Internet Explorer.
2. In **Location** , type `http://`, followed by the host name and FH Web Edition client installation page.

   Example: `http://hostname/fhweb/clients.html`

3. Follow the on-screen instructions to download and run the client setup program for your computer's operating system.

Launch FH Web Edition from the computer's start menu

1. Select the FH Web Edition menu option:

On this platform	Do this
Windows	• Choose **Start** → **Programs** → **ACSXerox** → **FH Web Edition 4** → **FH Web Edition**.
Linux	• Choose **Applications menu**→ **Network or Internet category** → **FH Web Editio**n.
Mac OS X	1. Select **Go** → **Applications**. 2. Double-click **FH_Web**.

2. In the **Connection** dialog box, type the address of the host.
3. Click **Connect**.
4. In the **Sign In** dialog box, type the network user name and password.

> **Note:** FH Web Edition allows users three invalid logon attempts before shutting down the logon process.

(Windows) Create a shortcut to a FH Web Edition server

On Windows computers, the FH Web Edition Connection dialog has an option to create a shortcut to a FH Web Edition server. You can use this option to bypass the Connection dialog when connecting to a host.

1. Start FH Web Edition.
2. In the **Connection** dialog box, type the address of the host.
3. Select **Create desktop shortcut to this host**.
4. Click **Connect**.

   A shortcut to the host appears on the desktop of the computer.

Launch FH Web Edition from a console window

1. Open a console window.
2. Type `FH_Web`.
3. In the **Connection** dialog box, type the server address.
4. Click **Connect**.

FH Web Edition startup parameters

FH Web Edition supports the following shortcut and hyperlink parameters.

Shortcut	Hyperlink	Description
`-u`	user	The name of the user's account.
`-p`	password	The user's password.
`-h`	host*	The network name of the FH Web Edition server.
`-hp`	port	The port on which the FH Web Edition server accepts connections. (By default, port 491.)
`-a`	app	The application to run. This may be a command-line string or the application name, as registered with the FH Web Edition Connection Manager.
`-r`	args	Application arguments.
`-c` or `-nc`	compression	`-c` or `compression = "true"` enables compression. `-nc` or `compression="false"` disables compression. (By default, `compression=true`.)
`-ac`	printerconfig	Determines how printers are initialized at startup. When `printerconfig ="all"` or `-ac` is followed by **all**, all printers are automatically configured. When `printerconfig = "none"` or `-ac` is followed by **none**, printers are not automatically configured. When `printerconfig = "default"` or `-ac` is followed by **default**, the default printer is configured automatically. This is the default setting.
`-f`	clientframe	When set respectively to `1` or *"true"*, all applications running in the session are displayed within a bounding window. When set respectively to `0` or `"false"`, applications are displayed within their own individual windows.
`-geometry`		The width and height of the client window. **Example:** `-geometry=800x600`
`-mm`	multimonitor	When set to `"true"`, the session's desktop spans all monitors. When set to `"false"`, applications are confined to the primary monitor. (By default, `multimonitor = "true"`.)
	width	The width of the frame or embedded window. (By default, 800.)
	height	The height of the frame or embedded window. (By

Shortcut	Hyperlink	Description
		default, 600).
	newWindow	When set to "true", applications run in a new browser window. When set to "false", applications run within the existing browser window. (By default, newWindow = "false".)
	embed	When set to "true", applications run within the browser window. When set to "false" applications run outside the browser window. (By default.embed = "true".)
	autoclose	When autoclose ="true", closing the Program Window closes the associated browser window and ends the user's FH Web Edition session. When autoclose ="false", closing the Program Window ends the user's FH Web Edition session, but does not close the browser window. (By default, autoclose ="false".)
	bInBrowser	bInBrowser only applies when the Plug-in is run in loose-windows mode. In this mode, when bInBrowser ="true", users are disconnected from their FH Web Edition sessions when they close the browser or browse to another page. In these cases, the session terminates on the host based on the host's timeout settings for disconnected sessions. When bInBrowser ="false", FH Web Edition runs in a separate process, and users are not disconnected from their sessions when they close the browser or browse to another page. (By default, bInBrowser ="true".)

*If no host is specified in the logon HTML page, FH Web Edition detects the machine from where the logon file was downloaded, and makes the connection to that host. The **Connection** dialog box does not appear,and the **Sign In** dialog only appears. If host= "?", users are prompted for the address of the host.

If an application is not specified, the Program Windows opens.

Note: If bInBrowser= "false" and autoclose ="true", the browser closes as soon as the session starts.

Create a FH Web Edition shortcut on Windows

1. Right-click the desktop, and then choose **New** → **Shortcut**.
2. In the **Create Shortcut** dialog box, browse to the FH Web Edition client executable file.

   Example:
   `"C:\Program Files\ACSXerox\FH Web Edition Client\FH_Web.exe"`

3. Add parameters after the path to FH_Web.exe.

   Example:
   `"C:\Program Files\ACSXerox\FH Web Edition\Client\FH_Web.exe" -h server-name -a Wordpad -r "C:\Users\Public\Public Documents\test.rtf"`

4. Type a name for the shortcut, and then click **Finish**.

Use shortcut parameters on Macintosh OS X

1. Open **Terminal**.
2. Navigate to `/Applications/FH_Web.app/Contents/MacOS/`.
3. Type `./ FH_Web` and append command-line arguments as needed

   Example: `./FH_Web -h 196.125.101.222 -c -ac all -hp 443`

Note:

- Parameters are optional and are not case-sensitive. They can be appended in any order, with the exception of `-r`. If `-r` is used, it must be the last parameter on the command line, and it must be used with the `-a` parameter.
- When the `-a` parameter is used, the Program Window is not launched, even if the application does not exist.
- Startup parameters passed on by the `-r` parameter are specific to each application. Refer to the application's documentation for information about its launch parameters.
- If a user does not have a password, `-p ""` can be used to bypass the **Sign In** dialog box, as long as the user name has also been specified in the shortcut.
- Parameters containing spaces must be enclosed in quotation marks.

  Example: The parameter `-a "Acrobat Reader"` launches Adobe's Acrobat Reader. Likewise, user name Jim C is specified as `-u "Jim C"`.

Create a FH Web Edition hyperlink

When FH Web Edition is run from a Web browser, FH Web Edition startup parameters can be specified by adding arguments to hyperlinks that reference the `logon.html` page. These hyperlinks can then be inserted into documents, Web pages, e-mails, instant messages, and so forth.

1. Open a Web page in an editor.
2. Choose the editor's **Insert Hyperlink** option.
3. Enter the address of the host, followed by the necessary hyperlink parameters.

   Example:
   ```
   http://hostname/logon.html?mode=embed&width=1024&height=768&
   app=C:\Program%20Files\Windows%20NT\Accessories\wordpad.exe&
   args=C:\Users\Public\Public%20Documents\test.rtf
   ```

   Note:
   - Parameters are optional and case-sensitive. They can be appended in any order.
   - Spaces within parameters must be replaced with "`%20`".

4. Save the page.

Resizing the client window

The command-line argument –geometry can be used to modify the size of the client window when the command-line argument –f is used. Without -geometry on the command-line, the client window will be maximized. When the FH Web Edition Client is run in loose window mode, -geometry has no effect.

- Append –geometry to the command-line, followed by the desired width and height.

  Example:
  ```
  ./FH_Web –h 196.125.101.222 –f –geometry800x600
  ```
  or
  ```
  ./FH_Web –h 196.125.010.222 –f –geometry=800x600
  ```

Uninstalling FH Web Edition

Instructions for uninstalling FH Web Edition depend on the platform and browser.

Uninstalling the FH Web Edition client from Windows

1. Open the **Control Panel**.
2. Double-click **Programs and Features**.
3. Select **FH Web Edition Client**.
4. Click **Change**.
5. Click **Next**.
6. Select **Remove**.
7. Click **Next**.
8. Click **Remove**.

Uninstalling the FH Web Edition client from Linux

1. Launch the Linux console.
2. Type `rpm -e FH_Web.linux`.
3. Remove the plug-in by typing:
   ```
   rm -rf ~/.mozilla/plugins/libnpg.so
   ~/.mozilla/plugins/libpbr.so > ~/.mozilla/ FH_Web
   ```
4. (If you plan to reinstall the plug-in) Clear the Firefox browser cache.

Uninstalling the FH Web Edition client on Macintosh OS X

1. Open **Terminal**.
2. Log on as `root`, using `su` and the `root` password.
3. Change to `/Applications/FH_Web.app/Contents/Utils/`.
4. Run the script by typing: `./Uninstall.sh`.
5. Close **Terminal**.

Uninstalling the FH Web Edition client from Firefox

1. Start Mozilla Firefox.
2. Choose **Tools** → **Addons**.
3. In the **ACS, A Xerox Company FH Web Edition** section, click **Uninstall**.
4. Close Mozilla Firefox.
5. Clear the Firefox browser cache.

Uninstalling the FH Web Edition client from Internet Explorer

1. Start Internet Explorer.
2. Choose **Tools** → **Internet Options** → **Programs** → **Manage add-ons**.
3. Select **FH Web Edition 4**.
4. (If there is a **Delete** button) Click **Delete**.
5. (If there is no **Delete** button) Do the following.
    a. Double-click **FH Web Edition 4**.
    b. Click **More Information**.
    c. Click **Delete**.
6. (If users have difficulty reinstalling and running the ActiveX Control) Clear the browser cache.
    a. Choose **Tools** → **Internet Options**.
    b. Click the **General** tab.
    c. Under **Temporary Internet Files**, click **Delete Files**.
    d. Have users check for any conflict directories.
        i. Open a command prompt window.
        ii. Type the location of the downloaded program files folder.
        iii. Check for any conflict directories.
        iv. (If any exist) Delete them.
        v. Close the command prompt window.

Uninstalling the FH Web Edition client from Apple Safari

1. Log on as `root`, using `su` and the `root` password.
2. Change to `/Applications/FH_Web.app/Contents/Utils/`.
3. Run the script by typing: `./Uninstall.sh`.
4. Close **Terminal**.

> **Note:** If users experience slow scrolling with FH Web Edition, try disabling the smooth scrolling option on the host. In Internet Explorer, choose **Tools** → **Internet Options**. Click the **Advanced** tab. In the **Settings** list, under **Browsing**, clear **Use smooth scrolling**.

Automatic client updates

Administrators can configure FH Web Edition to automatically update the FH Web Edition client when users connect to a FH Web Edition server that is running a newer version.

When clients are automatically being updated in the FH Web Edition Connection Manager, and a user signs in to the host from a Windows computer, FH Web Edition compares the version of the FH Web Edition client installed on the client computer to the version in the `Updates` directory on the host. If the files in the `Updates` directory are newer, FH Web Edition copies the newer files to a temporary directory on the client computer. When the FH Web Edition client then closes, the FH Web Update Client service installs the new files so they can be used in subsequent FH Web Edition sessions. Users are updated on the screen when the new updates complete installing.

A new FH Web Edition client is install through the update client service when the following conditions are met:

- Clients are automatically being updated in the FH Web Edition Connection Manager.
- The FH Web Edition Update client service is installed and enabled on the client computer.
- A newer version of the client is available in the `Updates` directory on the host.
- All of the files in the new version have been downloaded to the client computer.
- The user has signed out of his or her FH Web Edition client session.

Note:

- Automatic client updating for users running the ActiveX Control with Internet Explorer 6.0 is not supported.
- The default location for the Updates folder is `C:\Program Files\ACSXerox\FH Web Edition\Updates`, which is defined in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\ACSXerox\FH Web Edition\Updates`.

Enabling automatic client updates

1. Do one of the following.
   - (Windows) Install the FH Web Edition client on client computers using the `FH_Web.windows.exe` setup program.
   - (Macintosh and Linux) Download the updated client file from the FH Web Edition client installation page (Example: `http://hostname/fhweb/clients.html`) and install the appropriate client.
2. From the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Select **Automatically update clients**.
5. Click **OK**.

Updating the Mozilla Firefox plug-in

Users who have installed the plug-in with Mozilla Firefox can update the plug-in using Firefox's Add-on Manager.

1. In Firefox, choose **Tools** → **Add-ons**.
2. Click **Find Updates**.
3. Install the update.

Disabling the FH Web Edition Update Client service

Users are not required to perform any upgrade tasks. They can, however, prevent updates from being installed by disabling the FH Web Edition Update Client service on the client computer.

1. Right-click **My Computer**, and then choose **Manage**.
2. Choose **Computer Management** → **Services and Applications** → **Services**.
3. Select **FH Web Edition Update Client**.
4. Click **Properties**.
5. Under **Startup type**, select **Disabled**.
6. Click **Stop**.
7. Click **OK**.

Updating the ActiveX control and the plug-in

If FH Web Edition was deployed through a Web browser's Add-on manager, users should launch a Web browser to access a FH Web Edition Web server. The Web pages install and update the Web clients as long as the user has sufficient rights to install browser add-ons. If users have power-user rights, are running the ActiveX Control, and connect to a FH Web Edition server with an updated client, the ActiveX control updates automatically.

If the user does not have sufficient rights to install browser add-ons (the user is running Internet Explorer and is not an administrator or power user), the client should be installed using the FH Web Edition Client Setup Program.

Users who install the plug-in with Mozilla Firefox can update the plug-in through Firefox's Add-on manager.

Note: The Firefox plug-in update feature does not work if you install the native Windows Client. It only works when the Web client is installed through the Web browser page.

1. In Firefox, choose **Tools** → **Add-ons**.
2. Click **Find Updates**.
3. Install the update.

Windows CE client

To run the Windows CE client, devices must have TCP/IP as a network protocol. SEH (the C++ Structured Exception Handling component) and RTTI (the Run-Time Type Information component) are required to run FH Web Edition on a Windows CE device.

Determining if SEH and RTTI components exist on the device

1. In the Windows folder, open `ceconfig.h`.
2. Depending on your device, do one of the following.

Device	Do this

Windows CE 4	• Look for the following lines.
	`#define COREDLL_CRT_RTTI 1`
	`#define COREDLL_CRT_CPP_SEH 1`

Windows CE 5	• Look for the following line. `#define COREDLL_CRT_CPP_EH_AND_RTTI 1`

If the line(s) corresponding to your device exist in the file, RTTI and SEH are supported.

Installing the Windows CE client

Once the Windows CE client is installed, users can log on to a FH Web Edition server from the computer's start menu, from a desktop shortcut, or directly from the FH Web Edition executable.

Note: The Windows CE installation program attempts to delete `FH Web Edition.CAB` at the end of installation. As as result, you need to set the `FH Web Edition.CAB` file permission to read-only before installing it on the client device.

1. Start Internet Explorer.
2. In **Address**, type `http://`, followed by the host name and FH Web Edition client installation file.

   Example: `http://host/fhweb/clients.html`

3. Click the **Windows CE Client** link.
4. Determine which processor your Windows CE device is using and download the appropriate `.CAB` file (`ARMV4`, `ARMV4I`, or `X86`).
5. Double-click the `.CAB` file.

   The Windows CE client can be installed manually by launching `FH Web Edition.CAB` from the corresponding CPU folder on the client device.

   Example: `Web\Clients\FH Web Edition.CAB`

Running the Windows CE client from the Start menu

Users running CE devices with taskbar support can run the Windows CE client from the **Start** menu.

1. Choose **Start** → **Programs** → **FH Web Edition** → **FH Web Edition Client**.
2. In the **Connection** dialog box, type your host address.
3. Click **Connect**.
4. When the **Sign In** dialog box appears, enter the network user name and password.

Running the Windows CE client from a shortcut

On Windows CE devices with desktop shortcut support, a Windows shortcut named **FH Web Edition Client** is created during installation of the Windows CE client. This shortcut launches the Program Window.

1. Double-click the FH Web Edition Client shortcut.
2. In the **Connection** dialog box, type your host address.
3. Click **Connect**.
4. When the **Sign In** dialog box appears, enter the network user name and password.

Running the Windows CE client from the FH Web Edition executable

Users with CE devices that do not support the shortcut or **Start** menu launching options can run FH Web Edition directly from the FH Web Edition client executable.

1. Run `FH_Web.exe` on the client device.
2. In the **Connection** dialog box, type your host address.
3. Click **Connect**.
4. When the **Sign In** dialog box appears, enter the network user name and password.

Running FH Web Edition using command-line arguments

If a shortcut for FH_Web.exe can be created on the CE device's desktop, command-line arguments can be used to expedite the logon process. For example, the command-line arguments "-a" allows users to directly launch an application. Command-line arguments can also be used to pass on application specific startup parameters and to enable compression.

1. Right-click a **FH Web Edition** shortcut, and then click **Properties**.
2. On the **Shortcut** tab, place the cursor in the Target edit box and append any of the following command-line arguments after the quote (”):

Argument	Does this
`-h`	The FH Web Edition server address or host name.
`-u`	The client’s network user name.
`-p`	The client’s network password.
`-a`	The display name of the application to be launched. The application's display name should be identical to the application registered with the FH Web Edition Connection Manager.
`-r`	Startup parameters for the application.
`-hp`	Modifies the host port setting for the Application Publishing Service.
`-c` or `-nc`	`-c` enables compression, `-nc` disables compression. (Compression is enabled by default.)

Example:

```
...\FH_Web.exe" -h server -u username -p password -c -hp 443
```

Note:

- Startup parameters passed on by the `-r` argument are specific to each application. Please refer to the application’s documentation for information about launch parameters.
- Command-line arguments are optional and are not case sensitive. Arguments can be appended in any order, with the exception of `-r`. If `-r` is used, it must be the last argument on the command line, and it must be used with the `-a` argument.
- To accommodate spaces in user names, passwords, application display names, or application arguments, quotation marks must be included when using command-line arguments.

  Example: User name Jim C would be specified as `-u "Jim C"`.

Editing the name or command-line options of a connection

1. In the Terminal Connection Manager, on the **Configure** tab, select the connection you want to modify.
2. Click **Edit**.
3. Make changes to the name and command-line options for this connection.
4. Click **OK**.

Deleting a connection

1. In the Terminal Connection Manager, on the **Configure** tab, select the connection you want to delete.
2. Click **Delete**.

Running a FH Web Edition connection

1. In the Terminal Connection Manager, on the **Connections** tab, select the connection you want to run.
2. Click **Connect**.
3. In the **Connection** dialog box, type your host address.
4. Click **Connect**.
5. When the **Sign In** dialog box appears, enter the network user name and password.

Uninstalling the Windows CE Client

- Delete the following installation files from the directory on the client device to which you copied them:
  - `FH_Web.exe`
  - `clipc.dll`
  - `cs.dll`
  - `dc.dll`
  - `filec.dll`
  - `pbru.dll`
  - `sc.dll`
  - `scres.dll`
  - `sndc.dll`
  - `printc.dll`
  - `upc.dll`

Advanced topics

You can also perform load balancing, work with clients, and more with FH Web Edition.

Load balancing

Load balancing allows FH Web Edition sessions to be distributed across multiple hosts. Load balancing is required when the host resource requirements for a deployment exceed the capacity of a single host computer. Load balancing is done automatically, and is transparent to the user. FH Web Edition can also be used with any third party TCP/IP based load-balancing service.

Load balancing requires the following:

- A FH Web Edition server must be installed on each of the hosts in the cluster.
- For Web deployment, if the load balancer is balancing connections to both the Web server (Example: port 80) and the FH Web Edition server (Example: port 491), each of the FH Web Edition servers in the cluster must have a Web server running, and the Web server home directory should contain the FH Web Edition Web files. If the load balancer is only balancing connections to the FH Web Edition server, the FH Web Edition Web files do not need to be located on each FH Web Edition server. Web files can be installed on the machine running the Web server.
- If an application saves any user-specific settings in the registry, (Example: Corel WordPerfect, Microsoft Word, etc.) users should operate with roaming profiles rather than local profiles. Since there is no way of predicting which server the user will actually be logged onto in a balanced server farm, working with roaming profiles is the only way to ensure that user-specific settings are available to the user at all times.

A FH Web Edition server can be configured to operate as an independent host, a dependent host, or as a relay server.

Note: A relay server cannot be an application host.

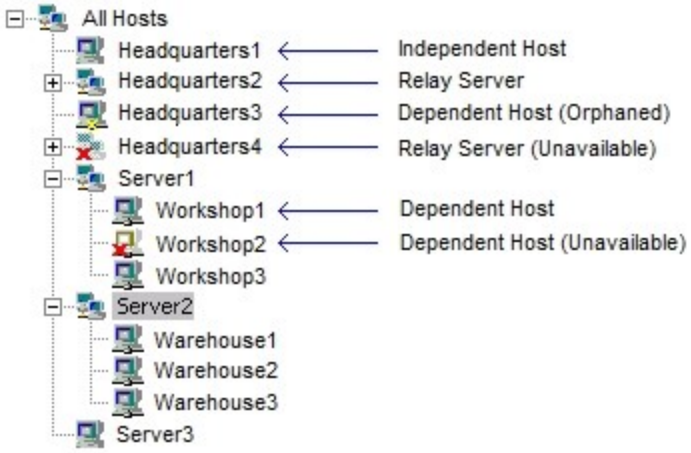
When setting up a load-balanced relay server configuration, you should use a license server. Information on license servers is available in:

- **Three-server redundancy**, on page 11.
- **License-file list redundancy**, on page 12.
- **Configuring FH Web Edition to use a central license server**, on page 14.

Independent hosts

Independent hosts are FH Web Edition servers that do not interact with other FH Web Edition servers running on the network. Independent hosts appear in the FH Web Edition Connection Manager on the first level of the FH Web Edition servers tree view as an independent node. The FH Web Edition setup program configures FH Web Edition servers to operate as independent hosts.

FH Web Edition clients can connect to independent hosts directly by specifying the name or IP address of the server in the **Connection** dialog box or the location box of a Web browser. Clients can also connect to independent hosts through a third-party network load balancer that distributes client connections among several servers. However, session reconnect is not supported in the latter configuration, and must be disabled.



Relay servers

A relay server is a FH Web Edition server that provides centralized control over one or more FH Web Edition servers. Relay servers maintain client connections and distribute FH Web Edition sessions across a set of load-balanced application hosts. Relay servers appear in the FH Web Edition Connection Manager on the first level of the **All Hosts** list as nodes with one or more dependent hosts.

After configuring a host to run as a relay server with one or more dependent hosts, FH Web Edition load-balances client connections and ensures that sessions start successfully. If a session fails to start on the selected host, the relay server selects another host and tries again until it finds one that can support the session.

Note:

- When setting up a relay server environment, be sure the same `Log Folder` path for the relay server exists on the dependent hosts. Otherwise, the **Sign In** dialog box does not appear when users attempt to sign in to FH Web Edition.

  Create a log directory on the `C:` drive of each relay server (Example: `C:\Data\APS_LOGS`), or use `C:\Program Files\ACSXerox\FH Web Edition\Log`, which already exists on the dependent host.
- Make sure this same path exists on the dependent host. In addition to changing the

`Log Folder` path in the Cluster Manger, the `\Log\Codes and \Log\Templates` directories must be copied to the new location.

- When a relay server is selected in the FH Web Edition Connection Manager, the number of processes running on all dependent hosts is not listed in the FH Web Edition Connection Manager's status bar.

A relay server requires a minimum of 512 MB of RAM. For most deployments and for best results, 1 GB with a multiprocessor server is recommended. Depending on the number of dependent hosts attached to the relay server, more RAM may be required.

Memory and CPU requirements for the dependent hosts are determined by the applications that are published and the number of users accessing the system. In general, a dependent host can support 12 “heavy” users/500 MHz CPU and 25 “light” users/500 MHz CPU. (“Heavy” is defined as a user running one or more large applications with continuous user interaction. “Light” is defined as a user running one application with intermittent user interaction.)

Configure a FH Web Edition server to operate as a relay server

1. From **All Hosts**, and then select the host you want.
2. Choose **Tools** → **Host Options**.
3. Click the **General** tab.
4. Type the name or IP address of the computer in **Relay server**.
5. Click **OK**.

   A message box appears, indicating that the change will not take effect until the FH Web Edition Application Publishing Service on the relay server has been restarted.
6. Click **OK**.
7. In the Control Panel, from the **Services** option, stop and restart the FH Web Edition Application Publishing Service.

Relay server failure recovery

On Windows hosts, the FH Web Edition Application Publishing Service can be configured to automatically restart if the service fails. If a relay server fails, clients are disconnected, but sessions continue to run on the FH Web Edition servers that were connected to the relay server. These servers attempt to reconnect to the relay server every 15 seconds. When a dependent host reconnects to the relay server, it re-adds its sessions to the relay server and restores any state information associated with the disconnected sessions. Clients are then able to sign back in and resume their sessions. Clients do not automatically attempt to reconnect to the relay server.

To provide higher service availability, a failover server can be configured for the FH Web Edition relay server using the Microsoft Cluster Service. In this configuration, if the relay server fails for any reason, the failover server immediately takes the place of the failed server. Application hosts automatically reconnect to the failover server, and users will generally be able to log on and reconnect to their disconnected sessions within one or two minutes of the relay server failure.

Dependent hosts

A dependent host is a FH Web Edition server that is connected to a relay server. FH Web Edition clients cannot connect directly to dependent hosts. Instead, they connect to the associated relay server, and the relay server selects one of the connected servers to host the session.

Users are authenticated on dependent hosts, not on relay servers. As a result, dependent hosts can be located on a different network than their associated relay server.

Example: Dependent hosts can be located behind a firewall on an internal, Active Directory network, and the associated relay server can be located in a demilitarized zone (DMZ) that is outside the firewall.

If integrated Windows authentication is used, clients and dependent hosts must be located on the same domain, but the relay server can be located on a different domain.

Note: You should install the same set of applications on each dependent host, using the same installation path.

Configure a FH Web Edition server to operate as a dependent host

1. From **All Hosts**, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **General** tab.
4. Type the name or IP address of the relay server in **Relay server**.
5. Click **OK**.

   A message box appears, indicating that the change will not take effect until the FH Web Application Publishing Service is restarted.
6. Click **OK**.
7. In the Control Panel, from the **Services** option, stop and restart the FH Web Edition Application Publishing Service.

   When the FH Web Application Publishing Service is restarted, the dependent host appears beneath the relay server in the FH Web Edition Connection Manager's list of FH Web Edition servers.

   A dependent host with a yellow x indicates that the host has been "orphaned;" (its relay server has gone down). If a host's icon has a red X, the administrator does not have administrative rights on the host. If the host's icon has a red X and is grayed out, the host is no longer running the Application Publishing Service or has been turned off. In any of these cases, the administrator is unable to access that host from the FH Web Edition Connection Manager.

Administering relay servers and dependent hosts on different networks

When a user starts the FH Web Edition Connection Manager on a relay server or a dependent host, the FH Web Edition Connection Manager connects to the relay server and attempts to authenticate the user using integrated Windows authentication. If the FH Web Edition Connection Manager is running on a dependent host and the associated relay server is located on a different network, a message such as the following is displayed:

```
Failed to log you on to Server8. This computer (Server4) and Server 8
may be located on different networks. Would you like to log onto
Server 8 and administer it remotely?
```

Clicking **No** returns you to the FH Web Edition Connection Manager, and its **All Hosts** list. Clicking **Yes** initiates a special remote administration session on the relay server as follows:

1. The FH Web Edition Connection Manager on the dependent host starts the FH Web Edition client.
2. The client connects to the relay server and starts a session.

   The **Sign In** dialog box appears to the user.
3. The user signs in, specifying the user name and password of an account that is a member of the Administrators group on the relay server.
4. The FH Web Edition Connection Manager starts on the relay server.

   The user can now administer the relay server and all of its dependent hosts. A maximum of two administration sessions can run on the relay server at any given time, regardless of the **Maximum sessions on this host** setting in the FH Web Edition Connection Manager, and regardless of license restrictions.

Dependent hosts inherit their list of published applications, server settings, and user settings from the relay server. Applications must be installed in the same directory on all dependent hosts.

Caution: Applications do not need to be installed on the relay server.

When a FH Web Edition server is connected to a relay server, all of its server settings are synchronized with those of the relay server. When any changes are made to the relay server's settings, they are also made to all hosts connected to that relay server. The only settings allowed to vary are the maximum number of sessions and the name of the relay server. All other settings in the **Host Options** and **Application Properties** dialog boxes are grayed out and cannot be modified.

When setting up a relay server, if an application is installed but not published on the dependent host, the application needs to be published on the relay server through the FH Web Edition Connection Manager.

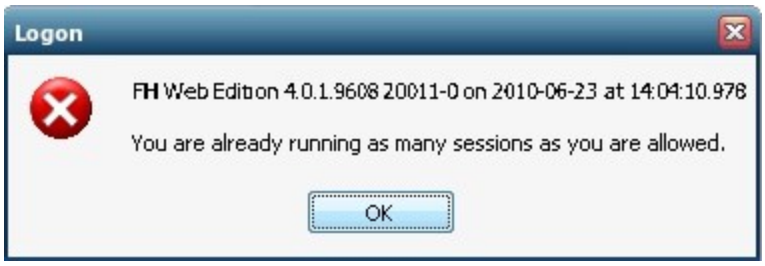
Example: Suppose Adobe Reader 7.0 is installed on the dependent host at `C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe`. You would need to open the FH Web Edition Connection Manager on the relay server, access the `Add Application` dialog box, and type this path location in **Executable Path**.

Note: Before publishing an item on a mapped drive, verify that the drive is mapped to the same drive letter and location on the dependent hosts as it is on the relay server.

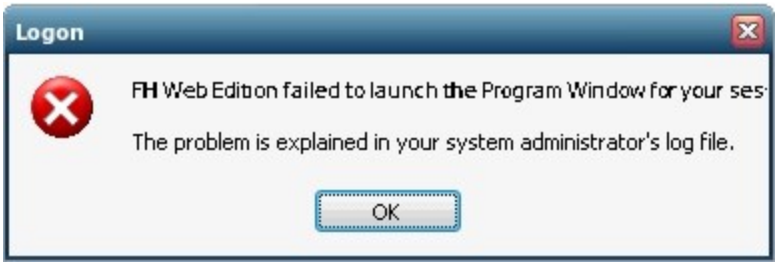
Host selection

When a client connects to a relay server, the relay server attempts to start a session on the dependent host that has the lowest number of running sessions as a percentage of the maximum number of sessions allowed for the host.

If the session fails to start on the selected host, the relay server successively attempts to start the session on other available hosts until it finds one that can support the session. If there are no available hosts (if the number of running sessions on **All Hosts** equals the maximum number allowed), the following message appears.


Logon
FH Web Edition 4.0.1.9608 20011-0 on 2010-06-23 at 14:04:10.978
You are already running as many sessions as you are allowed.
OK

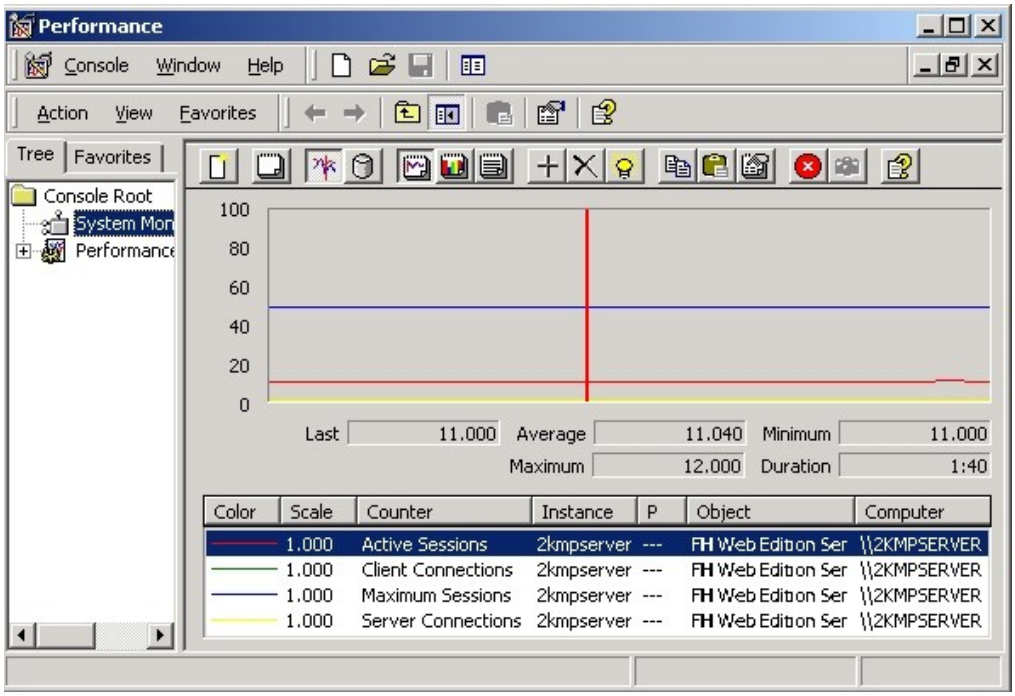
Otherwise, if the session cannot be started on any of the available hosts, the following message appears.


Logon
FH Web Edition failed to launch the Program Window for your ses
The problem is explained in your system administrator's log file.
OK

In a relay server setting, FH Web Edition checks the maximum sessions settings on the relay server and its dependent hosts. The maximum sessions value on the relay server is the maximum number of sessions that can be run concurrently on all dependent hosts assigned to that relay server. To modify the maximum sessions on this host, on the host, open the FH Web Edition Connection Manager, and then choose **Host Options → Session Startup**.

FH Web Edition server performance counters

FH Web Edition server performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a host. Performance counters can also be added to track the number of hosts connected to a relay server and to identify the maximum number of sessions allowed on a host. FH Web Edition server performance counters let administrators monitor host activity from any machine with network access to a FH Web Edition server.



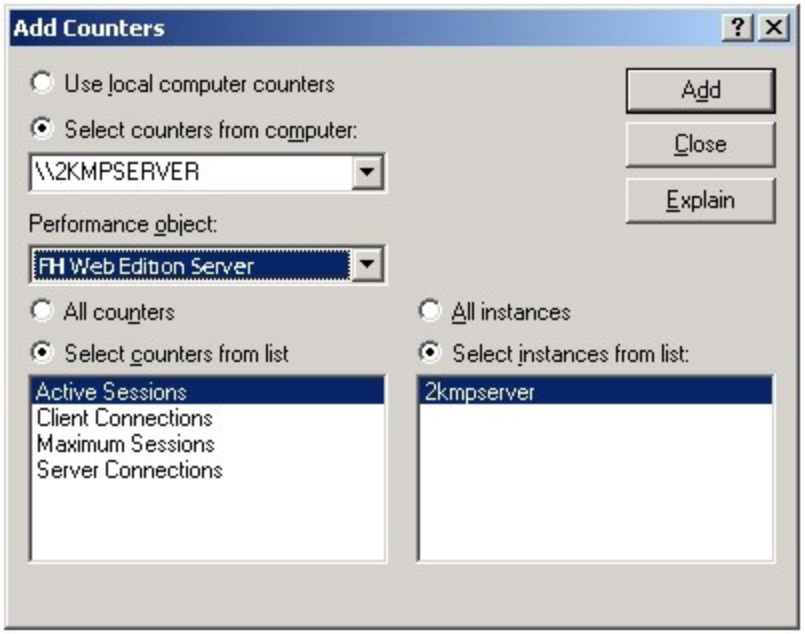
Note: The Remote Registry Service (`Regsvc.exe`) must be enabled for remote performance monitoring to work.

FH Web Edition server performance counters include:

- **Client Connections.** The total number of client connections on independent hosts or relay servers. This value is always zero for dependent hosts.
- **Server Connections.** The total number of dependent hosts connected to a relay server. This value is always zero for independent or dependent hosts.
- **Active Sessions.** For independent or dependent hosts, this is the number of sessions running on the host. For a relay server, this is the total number of sessions hosted on all connected dependent hosts.
- **Maximum Sessions.** This displays the maximum session count set in the FH Web Edition Connection Manager's **Host Options** dialog box.

Add FH Web Edition server performance counters to the Performance Monitor

1. Choose **Start** → **Programs** → **Administrative Tools** → **Performance**.
2. Click the **+** button to add counter(s).
3. From **Performance Object**, select **FH Web Edition Server**.



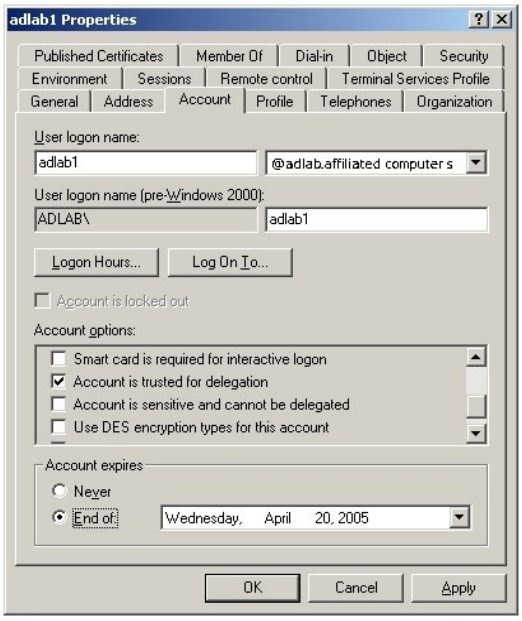
4. Select the counters you want (**Active Sessions**, **Client Connections**, **Maximum Sessions**, **Server Connections**).
5. Click **Add**.

Configuration requirements for delegation support

Network resource access and password caching on the host, as described under **Web Edition Connection Manager**, on page 25, require Windows delegation. The configuration requirements for delegation support are as follows:

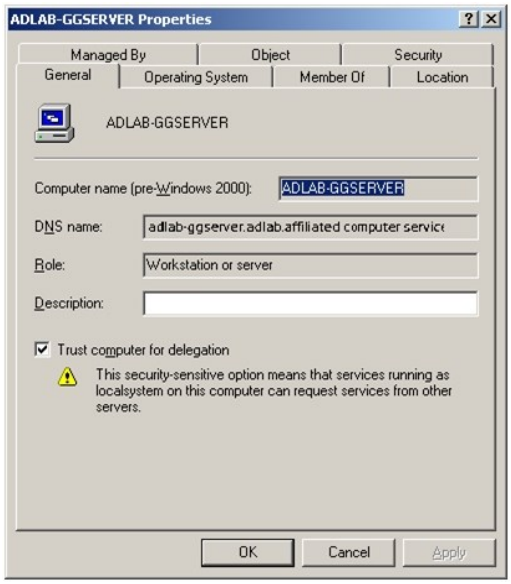
- Delegation requires the Kerberos authentication protocol and an Active Directory domain, both of which were introduced with Windows 2000. Host-side password caching and accessing shared folders using integrated Windows authentication are not supported from Windows NT 4.0 or Windows 98 client computers.
- The Domain Name System (DNS) servers must support Service Location (SRV) resource records. It is also recommended that DNS servers provide support for DNS dynamic updates. Without the DNS dynamic update protocol, administrators must manually configure the records created by domain controllers and stored by DNS servers. The DNS service provided with Windows 2000 or later supports both of these requirements.
- The computers hosting the FH Web Edition client, the FH Web Edition server, and any backend services, such as email or a database, must support Kerberos. Kerberos is supported by systems running Windows 2000 or later in a Windows 2000 or later Active Directory domain. FH Web Edition server is only supported on Windows 7 or later.
- The client's user account must support being delegated by the FH Web Edition Application Publishing Service.

    1. In the **Active Directory Users and Computers Management Console**, select the user and choose **Action** → **Properties**.
    2. Click the **Account** tab.
    3. Under **Account options**, scroll down and verify that **Account is sensitive and cannot be delegated** is cleared.
    4. Enable **Account is trusted for delegation**.



- The FH Web Edition server must have the right to delegate the user's account to other computers.

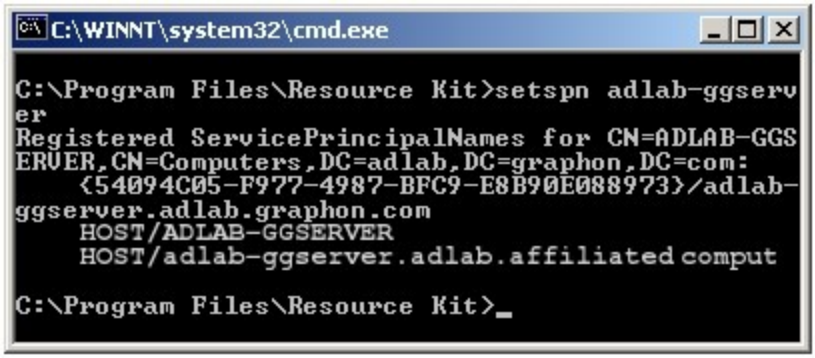
  1. In the **Active Directory Users and Computers Management Console**, select the computer.
  2. Choose **Action** → **Properties**.
  3. Enable **Trust computer for delegation**.



  The FH Web Edition Application Publishing Service must be configured to run in the local system account for these delegation rights to apply.

  > **Note:** After enabling Trust Computer for delegation in the Active Directory, the FH Web Edition server must be restarted in order for delegation to take effect.

- The FH Web Edition Application Publishing Service must be able to register its Service Principle Name (SPN) with Active Directory. It attempts to do this every time the service is restarted. The `setspn.exe` utility (available in the Microsoft Resource Kit and as a separate download from Microsoft) can be used to verify the SPN is properly set. The following command window shows output obtained from **setspn.exe** when run on the FH Web Edition server.



- Replace `adlab-ggserver` with the computer name of your FH Web Edition server. The `{54094C05-F977-4987-BFC9-E8B90E088973}` Globally Unique Identifier (GUID) is specifically used by the FH Web Edition Application Publishing Service to create the `{54094C05-F977-4987-BFC9-E8B90E088973}/adlab-ggserver.adlab.www.firehousesoftware.com` SPN.

  The following command window shows output obtained by running `setspn.exe` on the FH Web Edition server, and indicates a network configuration error. If all the above requirements are met, this should not occur.

Client printing

FH Web Edition supports client-side printing on all clients. By default, FH Web Edition automatically detects the client's default printer information once the user has signed in to the FH Web Edition server. This includes the default printer's port and printer driver. If the printer driver is not installed on the FH Web Edition server, FH Web Edition attempts to locate the driver and automatically install it.

When running applications on FH Web Edition servers, users can print to network printers and to printers that are directly connected to their computers, such as through serial, parallel, and USB ports.

Administrators can control which, if any, printers are available to users using the `-ac` and `printerconfig` FH Web Edition startup parameters.

When running FH Web Edition from a shortcut, use the `-ac` parameter with `all`, `none`, or `default`, to respectively make all, none or only the default printer available from applications running on the FH Web Edition server.

Example: To make all printers available, create a shortcut with the target specified as:
`"C:\Program Files\ACSXerox\FH Web Edition\Client\FH_Web.exe" -ac all`

Similarly, when running FH Web Edition from a hyperlink, use the `printerconfig` parameter with `all`, `none`, or `default`.

Example: The following hyperlink makes all printers available:
http://hostname/fhweb/logon.html?printerconfig=all

If no options are specified, FH Web Edition automatically configures the user's default printer only.

Note: The Print Spooler Service must be running on the FH Web Edition server to configure client printers.

Designating access to printer drivers

FH Web Edition can obtain printer drivers from the following sources:

- **Universal Printer Driver.** FH Web Edition includes a universal printer driver that can print to any client printer. Select **Universal Printer Driver** to allow the use of the Universal Printer Driver for configuring client printers.
- **Windows Printer Drivers.** Select **Windows Printer Drivers** to allow printers to be configured using already-installed native drivers. To allow FH Web Edition to automatically install native printer drivers that ship with Microsoft Windows, select **Automatically install drivers**.

When no options are selected, no printers are configured, and client printing is disabled. When only **Universal Printer Driver** is selected, the universal printer driver is used as a printer driver instead of native drivers. This is the default setting. When only **Windows Printer Drivers** is selected, only native printer drivers installed on the FH Web Edition server are used. If a printer's native driver is not installed, that printer is not configured.

When **Windows Printer Drivers** and **Automatically install drivers** are selected, only native printer drivers installed on the host, or those that are included with Windows, are used. If a printer's native driver is not installed and not included with Windows, that printer is not configured.

When both **Universal Printer Driver** and **Windows Printer Drivers** are selected, and a printer's native driver is installed on the host, the printer's native driver is used to configure the printer. If it is not installed on the host, the printer is configured to use the universal printer driver.

The universal printer driver is supported on Windows, Linux, and Mac OS X. Users running the Windows CE client must use the universal printer driver. When printing with the universal printer driver, the user (or group) needs to have full access to the `temp` directory.

A printer named `Preview PDF` is configured in each session when **Universal Printer Driver** is selected. Documents printed to this printer are automatically converted to a `.pdf` file and displayed on the client computer. Users can save, print, or email the document at their discretion. A PDF reader, such as Adobe Reader, is required on the client computer to use the universal printer driver's PDF conversion feature.

> **Note:** The universal printer driver uses a standard printing properties dialog box, and may not offer some of the more advanced printing options other drivers do.

Administrators set access to printer driver sources through the **Host Options** dialog box.

Designating access to printer drivers

1. In the FH Web Edition Connection Manager, from the **All Hosts** list, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Select **Printers**.
5. Select the driver source or sources you want.
6. Click **OK**.

Printer configuration

When FH Web Edition clients connect to a host, proxy printers are automatically created on the host and serve as an interface for printing to the client printer. Proxy printers are printers FH Web Edition sets up on the host as a bridge between the applications running in a FH Web Edition session and the client printers. Proxy printers can be configured automatically or manually.

Native printer drivers are preferred when configuring proxy printers, if they are available and if settings allow them to be used. Alternatively, the universal printer driver can be used when the native driver is not available. There are several methods an administrator can use to manage which printer drivers are used when creating proxy printers. Settings from client printers are replicated in their proxy printer counterpart. A session's proxy printers are removed when the session ends. Proxy printers are not removed when a session disconnects. All proxy printers on the system are removed when the Application Publishing Service starts.

When a proxy printer is configured, there is a hierarchy of preferences when selecting a native printer driver. In the FH Web Edition Connection Manager, if **Windows Printer Drivers** is cleared, this hierarchy is not applied. Native drivers are selected in the following order:

- **Printers Applet.** A user's manual selection of a printer driver in the Printers Applet takes precedence over all other driver selection methods.
- **Mapped Printer Drivers.** `MappedPrinterDrivers.xml` contains a list of driver names that can be used for each driver. This file is generated by the Application Publishing Service, but can also be manually edited by administrators.
- **Client driver name.** The driver with the exact name of the driver installed on the client is used to configure the proxy printer.

Printers Applet

FH Web Edition's Printers Applet lets users add and remove printers, edit printer properties, set the default printer, select a printer driver, and print test pages. The Printers Applet is accessible through the Program Window. It lists all the client printers that are configured and all the host printers that the user has access to. The list of printers depends on the printer drivers setting in the FH Web Edition Connection Manager, as well as the `-ac` and `printerconfig` parameters.

Settings made with the Printers Applet are saved the next time the user signs in to FH Web Edition. These settings take precedence over command-line options. Printer changes made in the Printers Applet take effect immediately. Users do not need to restart their session.

This applet icon	Indicates this
	The printer is installed on the client.
	The default printer, which is installed on the client.
	The printer is installed on the host.

This applet icon	Indicates this
	The default printer, which is installed on the host.

Adding and removing printers

Note: When a printer is added or removed through the Printers Applet, it does not add or remove it from the client computer—it only determines which printers are configured for use with FH Web Edition.

Adding a client printer

1. From the Program Window, choose **File** → **Printers**.
2. Click **Add**.
3. In the **Add Printer** dialog box, select the printer you want, and then click **Add**.

   This adds the printer to the list of configured printers, and it is now available for use.

   Note: When a printer is added through the Printers Applet, it is configured at startup regardless of the `-ac` command-line option or `printerconfig` parameter.

Removing a printer

1. From the Program Window, choose **File** → **Printers**.
2. From the list, select the printer you want.
3. Click **Remove**.

   Removing a printer from the list prevents it from being configured the next time the user starts a FH Web Edition session.

   Tip: The printer can be re-added to the list at any time by clicking **Add**, and then selecting it from the list.

Setting the default printer

Users can specify their default printer in the Printers Applet. The default printer is indicated by a black circle and checkmark above the printer. Any printer, including host printers, can be designated as the default.

1. From the Program Window, choose **File** → **Printers**.
2. From the list, select the printer your want to work with.
3. Click **Default**.

Editing printer settings

Through the Printers Applet, users can edit printer settings such as layout orientation and paper size.

1. From the Program Window, choose **File** → **Printers**.
2. From the list, select the printer your want to work with.
3. Click **Edit**.
4. Change the printer settings as needed.
5. Click **OK**.

Printing a test page

From the Printers Applet, users can print a test page to verify that the printer is properly configured and to check if a printer is printing graphics and text correctly. A test page also displays information such as the printer name, model, and driver software version, which may be helpful for troubleshooting printer problems.

1. From the Program Window, choose **File** → **Printers**.
2. From the list, select the printer your want to work with.
3. Click **Test Page**.

Changing a printer's driver

Through the Printers Applet, users can select different drivers for their printers. This is useful if a driver is not working properly or if a user wants to switch between native drivers and the universal printer driver.

Note: When only the universal printer driver is designated as a driver source in the FH Web Edition Connection Manager, users are unable to change drivers. Users cannot change the driver for FH Web Edition's Preview PDF printer, or for server-based printers.

1. From the Program Window, choose **File** → **Printers**.
2. From the list, select the printer your want to work with.
3. Click **Driver**.
4. In the **Select Printer Driver** dialog box, select a one of the drivers currently installed on the FH Web Edition server.
5. Click **OK**.

   The printer is configured with the new driver.

Resetting printer settings

At any time, users can reset printer data to its default settings, including preferences and printer settings. This may be useful if printers are not configuring properly, or if users are experiencing printer issues.

Caution: Resetting printer settings removes all proxy printers from the session. Users must restart their session to print to client printers again. This also resets the default printer to its original default setting.

1. From the Program Window, choose **File** → **Printers**.
2. Click **Reset Printers**.

Mapping printer drivers

Administrators can map printer drivers by editing the `MappedPrinterDrivers.xml` file. For most FH Web Edition deployments, administrators do not need to edit this file. It is used for specifying which driver to use when a host's driver name does not identically match the client's, or when the administrator wants to override native drivers and force clients to use a different printer driver or the universal printer driver.

Changing to a different printer driver

1. Navigate to `C:\ProgramData\ACSXerox` or to `C:\Documents and Settings\All Users\Application Data\ACSXerox` and locate the `MappedPrinterDrivers.xml` file.
2. Open the file in Wordpad and search for the client printer driver name.

   Example:

   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS</value>
   </property>
   ```

   `<property id="HP LaserJet 2100 Series PS" type="STRING">` is the driver used on the client, and `<value>HP LaserJet 2100 Series PS</value>` is the driver that should be mapped to on the host.
3. Replace the driver name in `<value>` with the new printer driver name.

   Example: In the example above, you would delete `HP LaserJet 2100 Series PS` and replace with the new printer driver.
4. Save the file.

   This change takes effect the next time the user starts a FH Web Edition session.

Forcing a printer to use the universal printer driver

Mapping printer drivers can also be used to force printers to use the universal printer driver.

1. Navigate to `C:\ProgramData\ACSXerox` or to `C:\Documents and Settings\All Users\Application Data\ACSXerox` and locate the `MappedPrinterDrivers.xml` file.
2. Open the file in Wordpad and search for the client printer driver name.

   Example:
   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS</value>
   </property>
   ```

   `<property id="HP LaserJet 2100 Series PS" type="STRING">` is the driver used on the client, and `<value>HP LaserJet 2100 Series PS</value>` is the driver that should be mapped to on the host.
3. Replace the driver name with `Universal Remote Printer`.

   Example: In the example above, you would delete `HP LaserJet 2100 Series PS` and replace it with `Universal Remote Printer`.

   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>Universal Remote Printer</value>
   </property>
   ```
4. Save the file.

   The next time users connect to the host, their printer is configured using the universal printer driver.

Designating an additional driver

Multiple drivers can be specified in the `<value>` field by delimiting them with a semicolon. Administrators can add an unlimited number of driver names. FH Web Edition attempts to configure client printers using the drivers in the order in which they are specified. The semicolon-separated drivers specify the preferential order of drivers to be used when installing a proxy printer.

1. Navigate to `C:\ProgramData\ACSXerox` or to `C:\Documents and Settings\All Users\Application Data\ACSXerox` and locate the `MappedPrinterDrivers.xml` file.
2. Open the file in Wordpad and search for the client printer driver name.

   Example:
   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS</value>
   </property>
   ```

`<property id="HP LaserJet 2100 Series PS" type="STRING">` is the driver used on the client, and `<value>HP LaserJet 2100 Series PS</value>` is the driver that should be mapped to on the host.

3. In `<value>`, add a semicolon and an additional driver name.

   Example: In the example above, you would add `;HP LaserJet 2200 Series PS` to the driver already in `<value>`.

   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS;HP LaserJet 2200 Series PS</value>
   </property>
   ```

4. Save the file.

Removing printer driver mapping

1. Navigate to `C:\ProgramData\ACSXerox` or to `C:\Documents and Settings\All Users\Application Data\ACSXerox` and locate the `MappedPrinterDrivers.xml` file.
2. Open the file in Wordpad and search for the client printer driver name.

   Example:

   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS</value>
   </property>
   ```

   `<property id="HP LaserJet 2100 Series PS" type="STRING">` is the driver used on the client, and `<value>HP LaserJet 2100 Series PS</value>` is the driver that should be mapped to on the host.

3. Delete the entire modified line.

   Example: You would delete all the lines in the example above.

4. Save the file.

   Tip: You can also delete the `MappedPrinterDrivers.xml` file to remove any prior changes. The file is recreated when users sign in to the host.

Note: Client printers are temporarily installed on the FH Web Edition server for the duration of the client's session. Printer drivers are installed permanently. Administrators can view the list of printers and drivers on the FH Web Edition server, in the `Printers` folder.

Information on adding adefault printer for all new users is available in *How to Add a Default Printer for All New Users*, at http://support.microsoft.com/support/kb/articles/Q252/3/88.ASP.

Client printer naming customization

FH Web Edition installs a printer on the host for each printer configured on the client machine. These printers are called proxy printers and are the printers seen by users when printing through FH Web Edition. Since multiple users connect to a FH Web Edition server, these printers must be filtered so that users see only their own printers. This requires that each printer be assigned a unique identifier.

Through the registry, administrators can specify the format of these proxy printer names and include information such as the user's name, the client computer's IP address, and the client machine name.

Administrators can choose from the following tokens to create a suffix to the printer string name.

Token	Description	Example
`%U`	User name	`Wilson`
`%I`	Client IP address	`192.168.100.147`
`%M`	Client's unique ID (GUID)	`800fb6b5770-ed9e-11df-82ae-000874b1cdb1`
`%C`	Client machine name	`HRWorkstation`
`%S`	FH Web Edition session ID	`7`

Customizing the client printer name

Caution: The following characters are not allowed in a client printer name: `! , \ = / : * ? " < >` and `|`. If any of these characters are used in the string, they are replaced with a hyphen. Any special characters other than `%` in the `PrinterNameFormat` string are taken literally, since they are not tokens.

1. Start the Registry Editor (`regedit.exe`).
2. In the Registry Editor, expand `HKEY_LOCAL_MACHINE`.
3. Locate the `PrinterNameFormat` key: `[HKLM\Software\ACSXerox\FH Web Edition\AppServer\PrinterNameFormat]`
4. Right-click `PrinterNameFormat`, and then select **Modify**.
5. In **Value**, type one or more of the client printer customization tokens.
6. Close the Registry Editor.

   The `PrinterNameFormat` key is set to (from %C) by default. Using the above examples, printer names would appear as: `PrinterName (from HRWorkstation)`.

Enabling client clipboard

FH Web Edition allows client and host-based applications to exchange information using the clipboard. Users can cut/copy information from applications running on the client, and paste it into applications running on a FH Web Edition server, and vice versa. Clipboard support is disabled by default.

1. In the FH Web Edition Connection Manager, from the **All Hosts** list, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Select **Clipboard**.
5. Click **OK**.

Enabling client sound, and client serial and parallel ports

FH Web Edition supports sound capability for any application that uses PlaySound, sndPlaySound, or waveOut. Sound cards must be installed on the host and client machines. Speakers are not required on the host, but are on the client machine. Audio support is disabled by default.

FH Web Edition also allows applications running on the host to access client machines' serial and parallel ports. Serial and parallel ports are disabled by default.

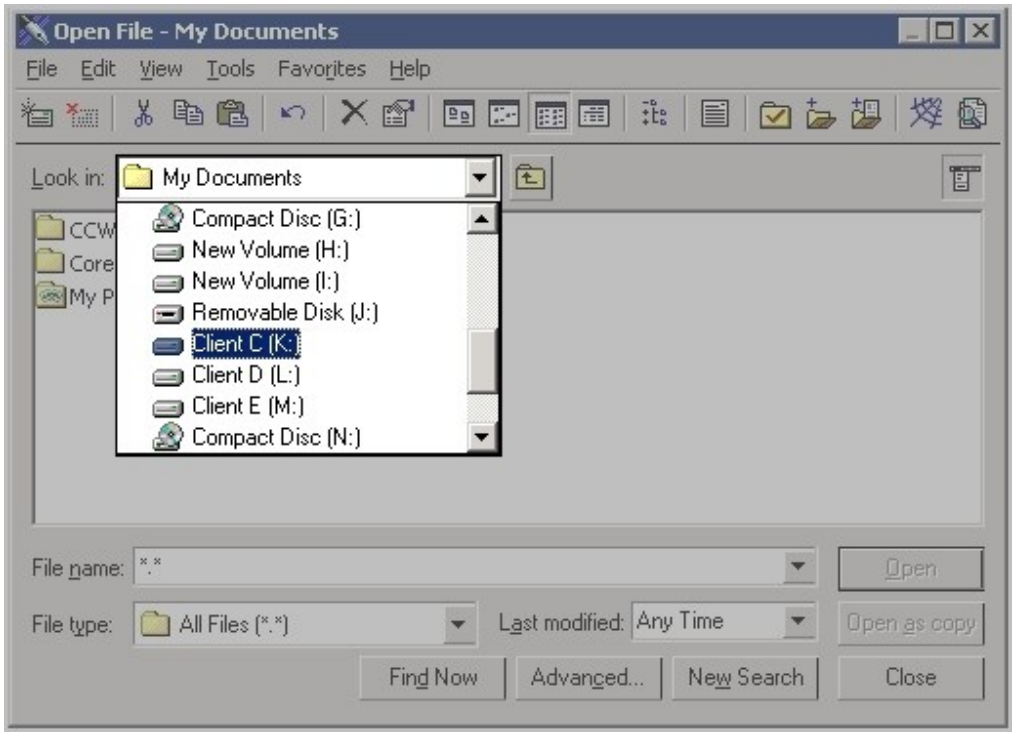
> **Note:** Client sound and client serial and parallel ports requires the loading of FH Web Edition libraries into session processes. This can affect the startup of a process, make some processes incompatible with FH Web Edition, or have fatal consequences during suspend/resume operations. Information on these options is available in **Advanced session process configuration**, on page 100.

1. In the FH Web Edition Connection Manager, from the **All Hosts** list, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Depending on what want to do, select one or both of the following options.
   - **Sound**.
   - **Serial and Parallel Ports**
5. Click **OK**.

Enabling client file access

FH Web Edition allows users to access files stored on the client computer and to save files locally. Client drives are listed in the application's Open and Save as dialog boxes, and are designated with a **Client** prefix.

Example: `Client C (K:),Client D (L:).`



Note: FH Web Edition allows users to access USB drives. Removable drives such a floppy disks, CD ROMs, and DVD-ROMs are not supported as client drives.

The dialog boxes list both client and host drives. Support for client drives is disabled by default.

1. In the FH Web Edition Connection Manager, from the **All Hosts** list, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Select **Drives**.
5. Click **OK**.

Remapping client drives

When applications are run in FH Web Edition sessions with the client drives feature enabled, FH Web Edition ensures there is a one-to-one mapping between drive letters and the drives of the client and host computers. If a drive on the client and a drive on the host are assigned the same drive letter, FH Web Edition assigns a new drive letter to one of the drives. Client drives can be remapped by either listing them sequentially, starting at a given drive letter, or by incrementing their drive letters by a specified value.

Listing client drives sequentially starting at a given drive letter

This feature is disabled by default.

1. In the FH Web Edition Connection Manager, from the **All Hosts** list, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Select **Drives**.
5. In **Assign consecutive letters starting at**, type the drive letter that should start the sequence.

   Example: If a client computer has A, C, D, and H drives, and the starting point is set to drive letter M, the client's drives are remapped respectively to M, N, O, and P. If a drive letter is already assigned to a drive, the next available letter is used. Once enabled, the default drive letter is M.

6. Click **OK**.

Incrementing client drive letters by a fixed value

1. In the FH Web Edition Connection Manager, from the **All Hosts** list, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Select **Drives**.
5. In **Increment by: ____ letters**, type a number greater-than or equal-to 1, that will yield the necessary offset.

   Example: If the client computer has A, C, D, and H drives, and the offset is 12, each of the client's drives are incremented by 12 letters. The drives are remapped respectively to M, O, P, and T. The default value for this setting is 12.

6. Click **OK**.

Hiding client drives

Through the FH Web Edition Connection Manager, administrators can hide client drives such as the client's operating system drive, floppy drive, and CD ROM drive, making them inaccessible to the user through FH Web Edition. All client drives are mapped by default.

1. In the FH Web Edition Connection Manager, from the **All Hosts** list, select the host you want to work with.
2. Choose **Tools** → **Host Options**.
3. Click the **Client Access** tab.
4. Select **Drives**.
5. In **Hide**, type the client drive letters you want to hide.

   Drives in **Hide** can be listed in any order. When hiding client drives on the Linux client and the Macintosh OS X Client, the user's home directory is mapped, in addition to the root and floppy drives.

   Example:
   ```
   Client Floppy (M:)
   Client Home (N:)
   Client Root (O:).
   ```
6. Click **OK**.

Hiding host drives

Microsoft's Group Policy Objects lets you hide specific host drives. Information on hiding host drives is available in Using Group Policy Objects to hide specified drives, at http://support.microsoft.com/kb/231289.

Note: To hide host drives, in the FH Web Edition Connection Manager's **Host Options** dialog box, **Apply Group Policy** must be enabled .

Mapped drives

Drive mappings are private within each FH Web Edition session.

Example: If there are two sessions running on a FH Web Edition server, a drive letter such as H, can be mapped to one network share in session one (`\\servername\session1`), and the same drive letter can be mapped to a different network share in session two (`\\servername\session2`).

You should use logon scripts to define drive letter mappings. You can also let users define their own drive letter mappings by publishing applications that provide this functionality.

Drive mappings defined within the interactive session on the FH Web Edition server are not available to remote users. If all users require access to the same network share through a drive mapping, the drive mapping needs to be defined in a logon script.

Multiple monitor support

The FH Web Edition Client supports multiple monitors on Windows. Multiple monitor support is enabled by default, but can be manually disabled.

To do this	Do this
Disable through a shortcut	Add the argument `-mm 0` to the shortcut **Example:** `FH_Web.exe -h server1 -mm 0`
Enable through a shortcut	Add the argument `-mm 1` to the shortcut **Example:** `FH_Web.exe -h server1 -mm 1`
Disable through a hyperlink	Set the `multimonitor` parameter to `false` **Example:** http://hostname/fhweb/logon.html?multimonitor=false
Enable through a hyperlink	Set the `multimonitor` parameter to `true` **Example:** http://hostname/fhweb/logon.html?multimonitor=true

Obtaining the name of the client computer

For applications that require the client's computer name rather than the FH Web Edition servers's, administrators can add the name of that executable under the registry key

`HKEY_LOCAL_MACHINE\SOFTWARE\ACSXerox\FH Web Edition\Compatibility\GetComputerName`

as a DWORD, with a data value of `0x00000001`. Any time an executable matching any of the names listed under this registry key with a data value of `0x00000001` calls the Windows `GetComputerName` API, the given buffer is filled in with the client's name rather than the host's name.

Additionally, there is an environment variable named `CLIENTCOMPUTERNAME` that exists as part of the running environment of a published application. This environment variable contains the client's computer name. The `CLIENTCOMPUTERIPADDRESS` environment variable performs the same function, except that it contains the IP address of the client computer, rather than the computer name. The standard Windows environment variable `COMPUTERNAME` remains unchanged; its value is the host's computer name.

1. Run the Registry Editor (`regedit.exe`).
2. In the Registry Editor, expand the `HKEY_LOCAL_MACHINE` key.
3. Locate the `GetComputerName` key `[SOFTWARE\ACSXerox\FH Web Edition\Compatibility\GetComputerName]`.
4. Create a DWORD entry for the executable.

   Example: `pw.exe`

5. Set the value of the new entry to `0x00000001`.
6. Close the Registry Editor.

Specifying the maximum color depth for FH Web Edition sessions

The color depth (or color quality) of a FH Web Edition session can affect the quality of images in some applications. FH Web Edition sessions run at the color depth of the client system up to a maximum value. By default, the maximum depth is set to 16-bits per pixel.

To increase or decrease the maximum color depth of a FH Web Edition session, use the `-mx` option when running FH Web Edition from a shortcut. The maximum color depth can be specified as follows: `-mx 32`, `-mx 24`, `-mx 16`, or `-mx 8`.

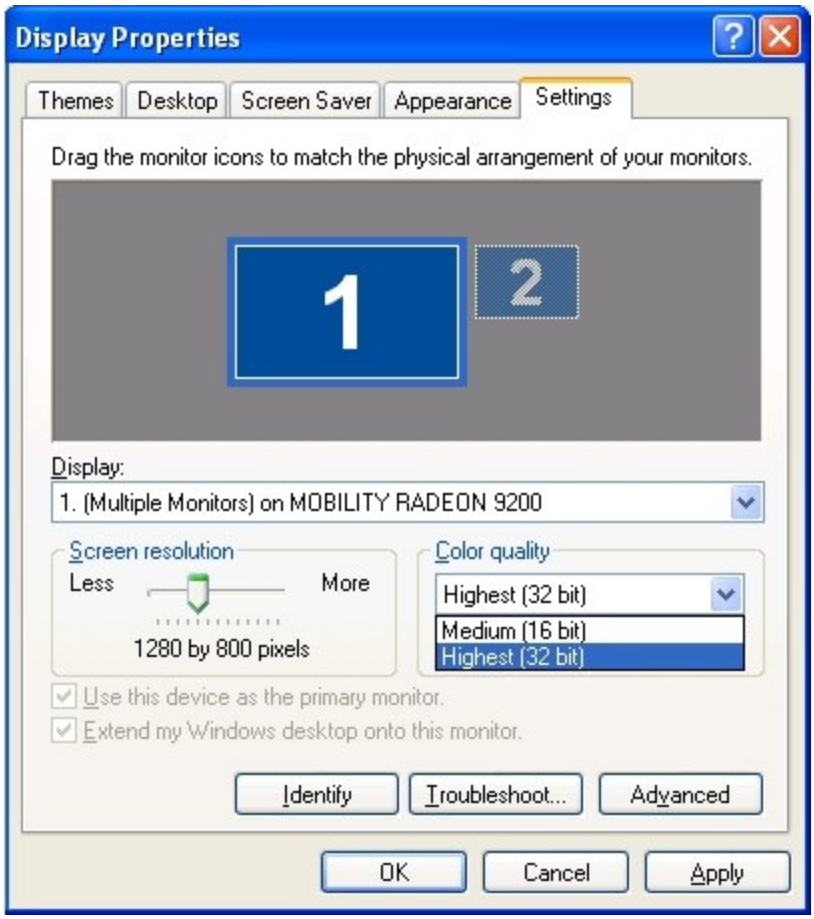
A FH Web Edition session uses the minimum value of the `-mx` option and the color depth of the client system.

Example: For a FH Web Edition session to run at 32-bits per pixel, `-mx 32` must be added to the command-line, and the client system must be running at 32-bits per pixel.

```
"C:\Program Files\ACSXerox\FH Web Edition\Client\FH_Web.exe" -mx 32
```

When running FH Web Edition from a hyperlink, use the `maxbpp` parameter with the values 8, 16, 24 or 32.

Example: The following hyperlink sets the maximum color depth to 24-bits per pixel:
http://hostname/fhweb/logon.html?maxbpp=24



Disabling image compression

By default, FH Web Edition compresses all images to a maximum of 256 colors per image. As a result, complex images may lose some sharpness. To disable image compression on FH Web Edition clients, append `-qt 0` to the shortcut as follows:

```
"C:\Program Files\ACSXerox\FH Web Edition\Client\FH_Web.exe" -qt 0
```

When running FH Web Edition from a hyperlink, set the `quantize` parameter to `false` to disable image compression.

Example: http://hostname/FH_Web_Edition/logon.html?quantize=false

Note: Disabling image compression may result in a significant increase in bandwidth sent from the FH Web Edition server.

Application script support

Many Win32 applications were designed for installation on a client PC and run by only one user. When an application is deployed from a FH Web Edition server, multiple users need to be able to run the application simultaneously, and a number of problems may be encountered if the application is not ready for multiple users.

You should modify the application so that it properly supports multiple users. When it is not possible to modify the application, an application script may be used to perform the pre-launch configuration and post-shutdown cleanup required to allow the application to run in a multiple-user environment.

1. Write a batch file that:
   - Performs the tasks necessary to prepare the application environment for a user.
   - Launches the application.
   - Performs any cleanup tasks required after the application shuts down. The batch file should end with an `EXIT` command, or the `CMD.EXE` process does not shut down.
2. Publish the application script.
   a. Open the FH Web Edition Connection Manager.
   b. Click **Tools** → **Applications** → **Add**.
   c. In **Application Path**, type the path to `CMD.EXE`.
   d. In **Command Line Options**, type `"/K` *filename*`"`, where *filename* is the full path of the batch file to be run.
   e. Type the application display name, and then specify an icon.
   f. Click **OK**.
3. Test the application script.
   a. Launch one of the FH Web Edition clients, and then connect to the FH Web Edition server.

b. Double-click the icon for the application script.

The user interface of the application appears on the client display, and the application runs in the environment configured by the application script.

> **Note:** When an application script is launched using FH Web Edition, the `CMD.EXE` window appears only briefly.The application script cannot contain any prompts for user input.

Advanced session process configuration

This section covers some of the advanced configuration options that can be set for processes running within FH Web Edition sessions. These settings can be applied to specific executable (`.exe`) applications, or as default settings applied to applications without specific configurations.

> **WARNING:** Care should be taken when making any changes discussed in this section. An incorrect configuration can affect the startup of a process, make a process incompatible with FH Web Edition, or have fatal consequences during suspend/resume operations.

Most applications that run within a FH Web Edition session have FH Web Edition libraries loaded within them to perform redirection to obtain the needed behavior. There are two levels of redirection that these libraries can initialize.

- The first level configures application and system modules to behave in a particular way. Most applications need one or more level-one settings enabled. Level-one settings include client time zone, client printing, and altered Windows API behavior.
- The second level creates a communications channel between the application and client for duplex transmission of session-related information. For the highest level of application compatibility with FH Web Edition, enable level-two settings in as few applications as possible. Level-two settings include client sound, and client serial and parallel ports.

The different configuration settings employed by the FH Web Edition libraries that redirect session processes are controlled by hexadecimal bit values within the registry. The desired bit values are logically ORed together to create a DWORD registry value. Below is the documented list of process redirector bits and a description of what they configure.

Redirector bit	Description
0x00000001*	Prohibits a process from running within a session.
0x00000002	Disables the loading of FH Web Edition libraries. All redirection is disabled. The time required to perform the redirection operations is a small percentage of the time required to launch typical Windows applications, but can be a large percentage of the time required to launch and run simple console applications. Some console applications do not require redirection, and performing these tasks can significantly extend the time required to execute logon scripts. Including this bit allows administrators to bypass redirection of a process. Applications execute faster since the FH Web Edition libraries are not loaded and initialized. This bit can also be used for applications that are incompatible with some or all of the FH Web Edition redirection settings.

Redirector bit	Description
0x00000004	Disables the client time zone. This bit can be used for applications that are incompatible with the FH Web Edition client time zone redirection settings.
0x00000008	Disables client printing. This bit can be used for applications that are incompatible with the FH Web Edition client printing redirection settings.
0x00000010*	Disables the use of the FH Web Edition 'UI' skin module.
0x00000020*	Enables the use of the FH Web Edition 'UI' skin module.
0x00000080*	Enables the Windows `ProcessIdToSessionId()` API to return the FH Web Edition session ID.
0x00000100*	On 64-bit systems, enables the Windows `ProcessIdToSessionId()` API to return the FH Web Edition session ID for 32-bit processes only. This is required for printing to work in 32-bit processes on 64-bit systems. **Note:** Including this bit in settings for 64-bit processes has no effect.
0x00000200	Disables client sound. This bit can be used for applications that are incompatible with the FH Web Edition client sound redirection settings.
0x00000400	Disables client serial and parallel ports. This bit can be used for applications that are incompatible with the FH Web Edition client serial and parallel ports redirection settings.
0x00000800*	Enables the Windows `GetComputerName()` API to return the client computer name. Additional information is available in **Obtaining the name of the client computer**, on page 97.
0x00001000*	Disables, for optimization purposes, some of the normal processing performed when `Explorer.exe` is launched. This bit prevents `Explorer.exe` from launching processes listed under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `RunOnce` and `RunOnceEx` registry keys. This reduces the system resources needed to run Explorer in a session.
0x80000000*	Enables application produced with Delphi to use the client serial and parallel ports feature. Applications built with Delphi do not properly process all return values from the Windows `GetOverlappedResult()` API. This bit prevents the returning of `WAIT_TIMEOUT`, and instead returns `WAIT_OBJECT_0`.

* Indicates advanced options that should only be used if instructed to by your support contact.

Note: All unlisted bits are purposely undocumented and reserved for internal use only. Do not alter any registry values that contain unlisted bits, and do not apply any unlisted bits to any registry values you add. FH Web Edition server operation will be compromised if this is done.

These bits can be combined to customize the redirector settings of specific applications or to change the default settings used by applications that do not have a registry entry.

Note: Always include the default value bits set by the initial installation of FH Web Edition, unless instructed otherwise by a support engineer.

Adding custom redirector settings for a specific application

1. Choose **Start** → **Run**.
2. Type: `regedit`
3. Browse to the registry key:
   `HKEY_LOCAL_MACHINE\ACSXerox\FH Web Edition\Loader\Processes`
4. Choose **Edit** → **New** → **DWORD value**.
5. Type the name of the application's executable file.

   Example: `beeps.exe`

   The application's name can be specified as either a fully qualified path or as the file's base name and extension.
6. Select the new registry value.
7. Choose **Edit** → **Modify**.
8. Verify that the base selection is hexadecimal.
9. In **Value data**, type the combined bits.
10. Click **OK**.

Changing the default redirection settings

1. Choose **Start** → **Run**.
2. Type: `regedit`
3. Browse to the registry key:
   `HKEY_LOCAL_MACHINE\ACSXerox\FH Web Edition\Loader\Processes`
4. Select the existing **DefaultLoaderOptions** registry value.
5. Choose **Edit** → **Modify**.
6. Verify that the base selection is hexadecimal.
7. In **Value data**, type the new setting.
8. Click **OK**.

Example configuration

A combination of application specific and the default settings can be used to minimize the risk of application incompatibilities, and allow an optimal environment to run in.

A FH Web Edition server has the following applications installed and registered in the FH Web Edition Connection Manager.

Application	Description
`DataDownloader.exe`	A Windows application that reads data from a serial device and saves it to a file. Client sound is needed for error conditions alerts that can be signaled while data is being downloaded. Client files access stores the data file on the client system. The Windows `GetComputerName()` API must be redirected so that the client computer name indicates the source of the data within the data file. Because the serial device that contains the data is connected to the client computer, client serial and parallel ports need to be enabled. Because this is the only process that accesses client serial and parallel ports on this system, a registry entry specifically for `DataDownloader.exe` is added. This minimizes the risks and overhead associated with this level-two redirector setting by disabling client serial and parallel ports in all other applications. The settings for this application are calculated as follows: • 0x00000110 - These are the bits originally set in `DefaultLoaderOptions`. • 0x00000800 - This is the bit that enables the Windows `GetComputerName()` API redirection. • 0x00000910 – This is the hexadecimal DWORD to be set in the `DataDownloader.exe` registry value.
`DataProcessor.exe`	A console application that needs client file access to read in the serial data file from the client and to write out the processed data file to the client. It also uses the client time zone to properly process the times recorded in the serial data file. All other settings are disabled to minimize the risks and overhead associated with redirector settings. The settings for this application are calculated as follows: • 0x00000110 - These are the bits originally set in `DefaultLoaderOptions`. • 0x00000008 - This is the bit that disables client printing. • 0x00000200 - This is the bit that disables client sound. • 0x00000400 - This is the bit that disables client serial and parallel ports. • 0x00000718 – This is the hexadecimal DWORD to be set in the `DataProcessor.exe` registry value.

Application	Description
DataViewer.exe	A Windows application that displays the data so that it can be analyzed. It needs client file access to read the processed data file from the client. It needs client sound so that application sounds can be heard. It needs client printing so that the analyzed data can be printed on paper. These are some of the settings needed by most applications, so the DefaultLoaderOptions registry value is used for the calculation below. The default setting is changed to disable the client serial and parallel ports. This can be done because the only application that uses client serial and parallel ports, DataDownloader.exe, has its own registry setting that specifically enables it. • 0x00000110 - These are the bits originally set in DefaultLoaderOptions. • 0x00000400 - This is the bit that disables client serial and parallel ports. • 0x00000510 – This is the hexadecimal DWORD to be set in the DefaultLoaderOptions registry value.

Proxy tunneling

Proxy tunneling via the `HTTP CONNECT` method lets a user who accesses the Internet through a proxy server connect to FH Web Edition servers on the Internet when the following conditions are met:

- The user runs the FH Web Edition client on a Windows computer.
- The address and port of the proxy server are stored under the client computer's Internet options.
- The proxy server is configured to allow `HTTP CONNECT` method tunnels to the port on which the FH Web Edition server is configured to accept `RapidX Protocol (RXP)` connections.

When users on Windows computers are unable to establish a direct connection to a FH Web Edition server, and when the client computer is configured through its Internet options to use a proxy server, FH Web Edition attempts to establish an `HTTP CONNECT` method tunnel to the FH Web Edition server.

Specifically, the client:

1. Connects to the proxy server using the address and port specified in the client computer's Internet options.
2. Sends a `CONNECT` request to the proxy server:

   Example: `CONNECT` *address:port* `HTTP/1.0`, where address and port are respectively the IP address of the FH Web Edition server, and the port on which the server accepts RXP connections (by default, 491).

3. Reads the reply from the proxy server.
4. Responds to the proxy server's reply as follows:
   a. If basic authentication is required, FH Web Edition prompts users for their user name and password, and then repeats step 2, this time providing the user's credentials.
   b. If the request failed, FH Web Edition displays the following message:

      ```
      Failed to connect to serverAddress via the proxy server at
      proxyAddress : [reason for failure].
      ```

   c. If the request succeeded, FH Web Edition initializes the RXP connection and starts the session.

Allowing HTTP CONNECT method tunnels using port 443

1. Configure the FH Web Edition server to accept connections on port 443.
2. Specify port 443 in the FH Web Edition hyperlink.
3. If necessary, configure the proxy server to allow connections to the FH Web Edition server on ports 80 (HTTP) and 443 (HTTPS).

   Once you have configured the FH Web Edition server and the FH Web Edition hyperlinks, users that meet the requirements are able to connect to the host.
4. (Users running FH Web Edition from a shortcut) Append the `-hp` argument followed by `443` to the shortcut.

   Example: `"...\FH_Web.exe" -h server -hp 443`

   Without `-hp 443` on the shortcut, these users are unable to sign in to FH Web Edition.

   Note:

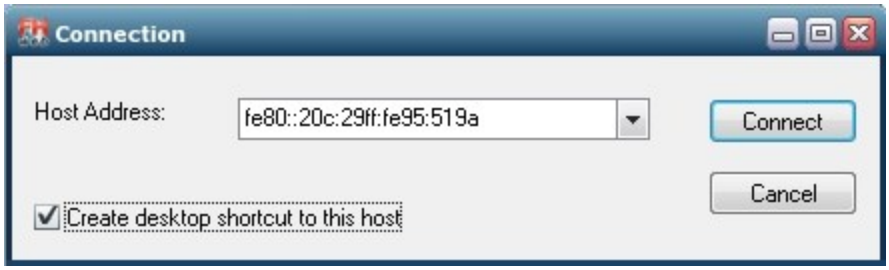
   - FH Web Edition clients are unable to connect to FH Web Edition servers through proxy servers configured to verify that the traffic on port 443 is HTTPS.
   - In a proxy server configuration, FH Web Edition only supports basic authentication.

Support for Internet Protocol version 6

FH Web Edition supports Internet Protocol version 6 (IPv6), the successor to IPv4, the dominant Internet layer protocol. IPv6 has a much larger address space than IPv4, and allows flexibility in allocating addresses and routing traffic.

FH Web Edition supports the following:

- FH Web Edition servers accept connections from IPv4 and IPv6 clients.
- FH Web Edition relay servers accept connections from IPv4 and IPv6 dependent servers.
- Administrators can specify a relay server in the FH Web Edition Connection Manager using a hostname, an IPv4 address, or an IPv6 address.
- Users can connect to a FH Web Edition server using its hostname, its IPv4 address, or its IPv6 address.



Enabling support for PAE

On Windows Server 2008, FH Web Edition supports memory in excess of 4 GB by way of the Physical Addressing Extension (PAE).

1. Click **Start** → **Run**.
2. Type `X:\boot.ini`, where X is the drive letter of the location of the boot files, `tldr`, `Boot.ini`, and so forth.
3. Modify the line that corresponds to your operating system by appending the switch `/PAE`.
4. Save the file.
5. Restart the computer.

Performance auto-tuning

Performance auto-tuning is used when an application is generating a large amount of graphical data or when a client system has limited processing speed. When performance auto-tuning is enabled, the client machine reports the rate at which it is processing the data the host is sending. The host uses this information to reduce the total amount of data it sends by eliminating any graphical information that the client system is unable to keep up with, such as animations with a high frame rate, or by choosing to send an image of an application's contents rather than primitive graphical operations.

Performance auto-tuning allows any client to run even the most graphically intense applications. Performance auto-tuning is disabled by default. You can enable performance auto-tuning for all clients connecting to a host.

1. Navigate to `C:\ProgramData\ACSXerox` and create a backup of the `HostProperties.xml` file.
2. In Wordpad, open `HostProperties.xml` and locate the following section:

```
</property>
- <property id="ClientProcessingBatch" group="Miscellaneous"
type="UINT32">
<value>0</value>
</property>
```

3. Change the `ClientProcessingBatch` value from `0` to `1`.
4. Stop and start the FH Web Edition Application Publishing Service.

Log files

The FH Web Edition server creates log files which record information about its own performance and that of certain FH Web Edition processes. Technical support uses the data to diagnose and correct problems that may arise. This can be especially helpful for errors that are only reproducible on specific machines or with a specific application.

All log files, whether they pertain to the client or host machine, are located in the `Log` folder on the FH Web Edition server.

Example: `D:\Program Files\ACSXerox\FH Web Edition\Log`

In the `Log` folder are three subfolders: `Backup`, `Codes`, and `Templates`.

Caution: Do not to delete these folders.

FH Web Edition messages are recorded within log files prefixed with `aps` and followed by the date and time (to the nearest millisecond) the Application Publishing Service was started.

Example: `aps_2011-04-04_09-55-47-636.html`

A new log file is created each time the Application Publishing Service is started. The log file with the latest date and time stamp contains messages for the current, or most recent instance of the Application Publishing Service.

Problems detected in the execution of FH Web Edition are described by entries in the log file. Each entry is uniquely identified by an item number along with a date and time stamp, and a description of the event or program error. Technical support uses this information to locate a problem's source and to determine its resolution.

Entries in the log file may also include prefixes for locating messages associated with an individual user's session and applications. If the event occurred within the context of a given session, the name of the session appears at the beginning of the message.

Example: `SuzyG on Server1`

If the event occurred within the context of a connection to the Application Publishing Service—a connection either from a client or from an application—the name of the connected process is included in the message prefix.

Example: `pw (1244)`

This message indicates that a problem occurred during the connection between the Program Window process and the Application Publishing Service. `1244` is the ID of the process in which the event took place.

If the message prefix contains the connection name `aps`, the event occurred within the Application Publishing Service, but was not associated with a connection to another process.

Selecting a new location for the log files

By default, log files are created and stored at `C:\Program Files\ACSXerox\FH Web Edition\Log`. You can select a new location for the log files.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Log**.
3. In **Folder** , type the path to the new directory, or browse to its location.

   Note: You cannot specify a path to a remote system for the log file location.

   Example: If you type a UNC path or a mapped network drive, the following message appearss:

   ```
   "Please specify a usable Windows folder where log files may be written."
   ```

4. Move the `Backup` folder and existing log files to the new location, along with the `Templates` and `Codes` subfolders.

Setting the output level

FH Web Edition offers six log output levels, as follows:

- 0: No output
- 1: Errors
- 2: Errors and events
- 3: Errors, events, and warnings
- 4: Errors, events, warnings, and diagnostic messages
- 5, 6: Errors, events, warnings, diagnostic messages, and trace messages

The default value for the output level is 1.

Caution: Setting the log output value to 5 or 6 causes the host to generate very large log files and may adversely affect performance and scalability. These output levels should only be used in a controlled environment—preferably when no clients are accessing the FH Web Edition server.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Log**.
3. In **Output level**, type one of the numeric values listed above
4. Click **OK**.

Maintaining log files

FH Web Edition creates a new log file in the `Log` folder every time the Application Publishing Service starts. Over time, these files can accumulate and consume a significant amount of disk space. To manage these files, FH Web Edition lets you delete or backup log files, and set file size or age limits.

Deleting log files

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Log**.
3. Under **Maintenance**, select **Delete**.
4. Specify how old (in days) log files can become before being deleted.
5. Specify at what size (in megabytes) log files are to be deleted.
6. Click **OK**.
7. Restart the FH Web Edition Application Publishing Service.

Backing up log files

Every half hour, and each time it is started, the Application Publishing Service searches the `Log` folder for files that have reached the specified age or size limit. It then either deletes the files or moves them to the `Log/Backup` folder. If, while sweeping the log files, the Application Publishing Service finds that the age or size limit has been met in the current log file, it closes the file and installs a newly created file in its place.

By default, log files are backed up after seven days, or when the file size has reached 20 MB.

1. In the FH Web Edition Connection Manager, choose **Tools** → **Host Options**.
2. Click **Log**.
3. Under **Maintenance**, select **Back up**.
4. Specify how old (in days) log files can become before being moved to the `Log/Backup` folder.
5. Specify at what size (in megabytes) log files are to be log files are to be moved to the `Log/Backup` folder.
6. Click **OK**.
7. Restart the FH Web Edition Application Publishing Service.